

(12)特許協力条約に基づいて公開された国際

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2005 年 2 月 3 日 (03.02.2005)

PCT

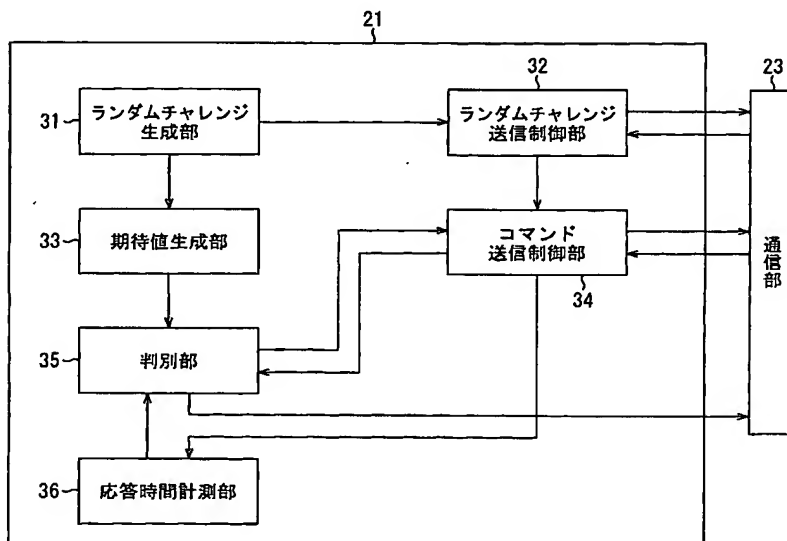
(10) 国際公開番号
WO 2005/010770 A1

- (51) 国際特許分類: G06F 15/00, H04L 9/32 (72) 発明者; および
(21) 国際出願番号: PCT/JP2004/009256 (75) 発明者/出願人 (米国についてののみ): 中野 雄彦
(22) 国際出願日: 2004 年 6 月 24 日 (24.06.2004) (NAKANO, Takehiko) [JP/JP]; 〒1410001 東京都品川
(25) 国際出願の言語: 日本語 区北品川 6 丁目 7 番 3 5 号 ソニー株式会社内 Tokyo
(26) 国際公開の言語: 日本語 (JP). 嶋 久登 (SHIMA, Hisato) [JP/JP]; 〒1410001 東京
(30) 優先権データ: (74) 代理人: 稲本 義雄 (INAMOTO, Yoshio); 〒1600023 東京
特願2003-281348 2003 年 7 月 28 日 (28.07.2003) JP 都新宿区 西新宿 7 丁目 1 1 番 1 8 号 7 1 1 ビル
(71) 出願人 (米国を除く全ての指定国について): ソニー ディング 4 階 Tokyo (JP).
株式会社 (SONY CORPORATION) [JP/JP]; 〒1410001 (81) 指定国 (表示のない限り、全ての種類の国内保護が
東京都品川区北品川 6 丁目 7 番 3 5 号 Tokyo (JP). 可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR,

[続葉有]

(54) Title: INFORMATION PROCESSING DEVICE AND METHOD, RECORDING MEDIUM, AND PROGRAM

(54) 発明の名称: 情報処理装置および方法、記録媒体、並びにプログラム



- 31...RANDOM CHALLENGE GENERATION SECTION
32...RANDOM CHALLENGE TRANSMISSION CONTROL SECTION
33...EXPECTATION VALUE GENERATION SECTION
34...COMMAND TRANSMISSION CONTROL SECTION
35...JUDGMENT SECTION
36...RESPONSE TIME MEASUREMENT SECTION
23...COMMUNICATION SECTION

(57) Abstract: There is provided an information processing device capable of appropriately communicating with a communication partner according to a communication time with the partner. A reception control section (41) receives a random challenge (RC) from a terminal (11) of a transmission side and supplies it to a generation section (42). The reception control section (41) transmits an RC reception message indicating that an RC has been received, to the transmission side. The generation section (42) subjects the RC to hash processing and supplies the authentication data obtained as a result to a generation section (43). At a timing before receiving a response request command from the transmission side, a transmission control section (44) controls the generation section (43) so as to generate a response message containing authentication data corresponding to the response request command and, upon reception of the response request command, transmits the response message to the terminal of the transmission destination. The present

invention can be applied to a content providing system.

(57) 要約: 本発明は、相手との通信時間に基づいて、通信相手と適切に通信することができるようにした情報処理装置に関する。受信制御部 41 は、送信側の端末 11 からのランダムチャレンジ (RC) を受信し、生成部 42 に供給する。受信制御部 41 は RC を受信した旨を表す RC 受信メッセージを送信側に送信する。生成部 42 は、RC に対してハッシュ処理を施し、その結果得られた認証データを生成部 43 に供給する。送信制御部 44 は、送信側からの応答要求コマンドを受信する前のタイミングで、生成部 43 を制御して、応答要求コマンドに

[続葉有]

WO 2005/010770 A1



BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG,

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明細書

情報処理装置および方法、記録媒体、並びにプログラム

技術分野

- 5 本発明は、情報処理装置および方法、記録媒体、並びにプログラムに関し、特に、通信相手との通信時間を適切に計測することができるようにした情報処理装置および方法、記録媒体、並びにプログラムに関する。

背景技術

- 10 近年、インターネットに代表される公共性のある広域に亘るネットワーク（以下、WAN(Wide Area Network)と称する）や一般家屋等に設けられる局所的なネットワーク（以下、LAN(Local Area Network)と称する）の普及に伴い、それらのネットワークを介した各種データ通信が盛んに行われている。

- 15 映像や音楽コンテンツなどを、ネットワークを通して伝送する場合は、著作権保護のために、通信相手の機器との間で、認証および鍵交換を行い、コンテンツを暗号化して伝送することが行われている（下記の文献参照）。

DTCP Specification Volume 1 Version 1.3 (Information Version)
http://www.dtcp.com/data/info_20040107_dtcp_Vol_1_1p3.pdf

- 20 ここにおいて、著作権の観点からは、家庭内でのコピーや伝送は許可するが、WAN で接続された他の家庭との間でのコンテンツの伝送を制限したい場合がある。例えば、テレビジョン放送を録画したコンテンツは、私的利用の範囲（家庭内）で利用できるが、インターネットを通して、他人に伝送するのは著作権を侵害すると考えられるので、このような制限が必要となる。

- 25 この制限の下では、著作権保護されたコンテンツを送信する機器（送信機器）は、そのコンテンツを受信する通信相手の機器（受信機器）が同一 LAN 内にあるか、WAN(インターネット)を通して接続されているかを判断する必要がある。

例えば、IP アドレスから通信相手が同一サブネット内にあるかどうかを調べる

ことや、IP 通信パッケージが通過した IP ルータの数 (Hop Count) を使うことで通信相手が WAN (インターネット) を通して接続されているかを知ることができる。

しかしながら、WAN (インターネット) を経由した通信であっても VPN (Virtual Private Network) などの技術を使えば、IP ルータを経由せずに接続されている同一サブネットであるかのように接続することが可能である。すなわち不正にコンテンツを入手することが可能である。

発明の開示

本発明はこのような状況に鑑みてなされたものであり、所定のコマンドに対する受信機器の応答時間に基づいて通信距離を判別し、例えば送信機器と同一 LAN に接続されているか否かを判定することを目的とする。

本発明の第 1 の情報処理装置は、受信装置との間で共有する共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信手段と、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置を認証する認証手段と、受信装置からの、コマンドに対する応答時間を計測する計測手段と、認証手段による認証結果、および計測手段により計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定手段とを備えることを特徴とする。

コマンド送信手段は、データの送信可否を判定するのに、コマンドを最大 N 回送信し、認証手段は、コマンドの送信の順番に応じた認証データとその期待値とに基づいて、受信装置を認証することができる。

本発明の第 1 の情報処理方法は、受信装置との間で共有する共有データに基づいて認証データが生成された後、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置を認証する認証ステップと、受信装置からの、コマンドに対する応答時間を計測する計測ステップと、認証ステップでの認証結果、および計測ステップの処理で計測された応答時間に基づい

て、受信装置に対するデータの送信可否を判定する判定ステップとを含むことを特徴とする。

本発明の第1の記録媒体のプログラムは、受信装置との間で共有する共有データに基づいて認証データが生成された後の、応答を要求するコマンドの受信装置
5 に対する送信を制御するコマンド送信制御ステップと、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づく受信装置の認証を制御する認証制御ステップと、受信装置からの、コマンドに対する応答時間の計測を制御する計測制御ステップと、認証制御ステップでの認証結果、および計測制御ステップの処理で計測された応答時間に基づく、受信装置に対するデータ
10 の送信可否の判定を制御する判定制御ステップとを含むことを特徴とする。

本発明の第1のプログラムは、受信装置との間で共有する共有データに基づいて認証データが生成された後の、応答を要求するコマンドの受信装置に対する送信を制御するコマンド送信制御ステップと、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づく受信装置の認証を制御
15 する認証制御ステップと、受信装置からの、コマンドに対する応答時間の計測を制御する計測制御ステップと、認証制御ステップでの認証結果、および計測制御ステップの処理で計測された応答時間に基づく、受信装置に対するデータの送信可否の判定を制御する判定制御ステップとを含む処理をコンピュータに実行させることを特徴とする。

20 本発明の第1の情報処理装置および方法、並びにプログラムにおいては、受信装置との間で共有する共有データに基づいて認証データが生成された後、応答を要求するコマンドが受信装置に送信され、共有データに基づいて生成された期待値と、受信装置において生成された認証データに基づいて受信装置が認証され、受信装置からの、コマンドに対する応答時間が計測され、認証結果、および応答
25 時間に基づいて、受信装置に対するデータの送信可否が判定される。

本発明の第2の情報処理装置は、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データを生成する認証データ生成

手段と、認証データ生成手段により生成された認証データを含む、コマンドに対する応答メッセージを、送信装置からコマンドが送信されてくる前に生成する応答メッセージ生成手段と、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージを送信装置に送信する送信手段とを備えることを特徴とする。

- 5 共有データは、疑似乱数であるようにし、疑似乱数は、コマンドの前に送信装置から送信されるようにし、認証データ生成手段は、疑似乱数に対して鍵付きハッシュ処理を施し、その結果得られたハッシュ値を認証データとすることができる。

- 10 認証データ生成手段は、疑似乱数と情報処理装置固有の情報に対して、鍵付きハッシュ処理を施し、その結果得られたハッシュ値を認証データとすることができる。

- データの送信可否を判定するのに、送信装置から、コマンドが最大N回送信されてくる場合において、認証データ生成手段は、送信装置から最初のコマンドが送信されてくる前に、共有データに対して処理を施して、送信されてくるN個の
15 コマンドのそれぞれに対応するN個の認証データを生成し、送信手段は、N個の認証データが、送信装置と予め合意した順番で送信装置に提供されるように、応答メッセージ生成手段により生成された応答メッセージを送信装置に送信することができる。

- 20 認証データ生成手段は、共有データに対して処理を施して得られたデータを複数個に分割し、分割されたデータからN個の認証データを生成することができる。

認証データ生成手段は、共有データに対して処理を繰り返し施し、その処理毎に得られたデータから、N個の認証データを生成することができる。

- 送信手段は、送信装置からのコマンドが受信されたとき、認証データとコマンドに含まれる情報から生成された新たな認証データを含む応答メッセージを、
25 送信装置に送信することができる。

本発明の第2の情報処理方法は、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データを生成する認証データ生成

ステップと、認証データ生成ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージを、送信装置からコマンドが送信されてくる前に、生成する応答メッセージ生成ステップと、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージを送信装置に送信する送信ステップとを含むことを特徴とする。

本発明の第2の記録媒体のプログラムは、送信装置からコマンドが送信されてくる前の、共有データに対して所定の処理を施しての認証データの生成を制御する認証データ生成制御ステップと、送信装置からコマンドが送信されてくる前の、認証データ生成制御ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、送信装置から送信されてきたコマンドが受信されたときの、応答メッセージの送信装置に対する送信を制御する送信制御ステップとを含むことを特徴とする。

本発明の第2のプログラムは、送信装置からコマンドが送信されてくる前の、共有データに対して所定の処理を施しての認証データの生成を制御する認証データ生成制御ステップと、送信装置からコマンドが送信されてくる前の、認証データ生成制御ステップの処理で生成された認証データを含む、コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、送信装置から送信されてきたコマンドが受信されたときの、応答メッセージの送信装置に対する送信を制御する送信制御ステップとを含むことを特徴とする。

本発明の第2の情報処理装置および方法、並びにプログラムにおいては、送信装置からコマンドが送信されてくる前に、共有データに対して所定の処理を施して、認証データが生成され、送信装置からコマンドが送信されてくる前に、生成された認証データを含む、コマンドに対する応答メッセージが生成され、送信装置から送信されてきたコマンドが受信されたとき、応答メッセージが送信装置に送信される。

本発明の第3の情報処理装置は、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成手段と、コ

マンド認証データを含み、応答を要求するコマンドを受信装置に送信するコマンド送信手段と、コマンドに対する受信装置からの応答を受信する応答受信手段と応答期待値と、受信装置から受信した応答に含まれる応答認証データに基づいて受信装置を認証する認証手段と、受信装置からの、コマンドに対する応答時間を計測する計測手段と、認証手段による認証結果、および計測手段により計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定手段とを備えることを特徴とする。

10 コマンド送信手段は、データの送信可否を判定するのに、コマンドを最大 k 回送信し、認証手段は、コマンドの送信の順番に応じた認証データとその期待値とに基づいて、受信装置を認証することができる。

15 本発明の第3の情報処理方法は、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、コマンド認証データを含み、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、コマンドに対する受信装置からの応答を受信する応答受信ステップと、応答期待値と、受信装置から受信した応答に含まれる応答認証データに基づいて受信装置を認証する認証ステップと、受信装置からの、コマンドに対する応答時間を計測する計測ステップと、認証ステップの処理での認証結果、および計測ステップにより計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定ステップとを含むことを特徴とする。

20 本発明の第3の記録媒体のプログラムは、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、コマンド認証データを含み、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、コマンドに対する受信装置からの応答を受信する応答受信ステップと、応答期待値と、受信装置から受信した応答に含まれる応答認証データに基づいて受信装置を認証する認証ステップと、受信装置からの、コマンドに対する応答時間を計測する計測ステップと、認証ステップの処理での

25

認証結果、および計測ステップにより計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定ステップとを含むことを特徴とする。

本発明の第3のプログラムは、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、
5 コマンド認証データを含み、応答を要求するコマンドを受信装置に送信するコマンド送信ステップと、コマンドに対する受信装置からの応答を受信する応答受信ステップと、応答期待値と、受信装置から受信した応答に含まれる応答認証データに基づいて受信装置を認証する認証ステップと、受信装置からの、コマンドに対する応答時間を計測する計測ステップと、認証ステップの処理での認証結果、
10 および計測ステップにより計測された応答時間に基づいて、受信装置に対するデータの送信可否を判定する判定ステップとを含む処理をコンピュータに実行させることを特徴とする。

本発明の第3の情報処理装置および方法、並びにプログラムにおいては、受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データが生成され、コマンド認証データを含み、応答を要求するコマンドが受信装置
15 に送信され、コマンドに対する受信装置からの応答が受信され、応答期待値と、受信装置から受信した応答に含まれる応答認証データに基づいて受信装置が認証され、受信装置からの、コマンドに対する応答時間が計測され、認証結果、および応答時間に基づいて、受信装置に対するデータの送信可否が判定される。

20 本発明の第4の情報処理装置は、送信装置との間で共有する共有データから、送信装置において共有データから生成されたコマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成手段と、送信装置から送信されてきたコマンドが受信されたとき、コマンドに含まれるコマンドの認証データと、生成手段により生成されたコマンド期待値データに基づいて送信装置
25 を認証する認証手段と、認証手段による認証結果に基づいて、応答認証データを含む応答を送信装置に送信する送信手段とを備えることを特徴とする。

本発明の第4の情報処理方法は、送信装置との間で共有する共有データから、送信装置において共有データから生成されたコマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、送信装置から送信されてきたコマンドが受信されたとき、コマンドに含まれるコマンドの
5 認証データと、生成ステップの処理で生成されたコマンド期待値データに基づいて送信装置を認証する認証ステップと、認証ステップの処理での認証結果に基づいて、応答認証データを含む応答を送信装置に送信する送信ステップとを備えることを特徴とする。

本発明の第4の記録媒体のプログラムは、送信装置との間で共有する共有データから、送信装置において共有データから生成されたコマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、送信装置から送信されてきたコマンドが受信されたとき、コマンドに含まれるコマンドの認証データと、生成ステップの処理で生成されたコマンド期待値データに基づいて送信装置を認証する認証ステップと、認証ステップの処理での認証結
10 果に基づいて、応答認証データを含む応答を送信装置に送信する送信ステップとを含むことを特徴とする。

本発明の第4のプログラムは、送信装置との間で共有する共有データから、送信装置において共有データから生成されたコマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、送信装置
20 から送信されてきたコマンドが受信されたとき、コマンドに含まれるコマンドの認証データと、生成ステップの処理で生成されたコマンド期待値データに基づいて送信装置を認証する認証ステップと、認証ステップの処理での認証結果に基づいて、応答認証データを含む応答を送信装置に送信する送信ステップとを含む処理をコンピュータに実行させることを特徴とする。

25 本発明の第4の情報処理装置および方法、並びにプログラムにおいては、送信装置との間で共有する共有データから、送信装置において共有データから生成されたコマンドの認証データに対応するコマンド期待値データおよび応答認証デー

タが生成され、送信装置から送信されてきたコマンドが受信されたとき、コマンドに含まれるコマンドの認証データと、生成されたコマンド期待値データに基づいて送信装置が認証され、その認証結果に基づいて、応答認証データを含む応答が送信装置に送信される。

5

図面の簡単な説明

図 1 は、本発明を適用した情報通信システムの利用例を示す図である。

図 2 は、図 1 の端末の構成例を示すブロック図である。

図 3 は、図 2 の送信可否判定部の構成例を示すブロック図である。

10 図 4 は、図 2 の応答制御部の構成例を示すブロック図である。

図 5 は、送信可否判定処理および応答処理を説明するフローチャートである。

図 6 は、期待値および認証データの生成方法を説明する図である。

図 7 は、期待値および認証データの他の生成方法を説明する図である。

図 8 は、図 1 の端末の動作を説明する図である。

15 図 9 は、図 2 の送信可否判定部の他の構成例を示すブロック図である。

図 10 は、図 2 の応答制御部の他の構成例を示すブロック図である。

図 11 は、他の送信可否判定処理を説明するフローチャートである。

図 12 は、他の応答処理を説明するフローチャートである。

図 13 は、図 1 の端末の動作を説明する他の図である。

20 図 14 は、図 1 の端末の動作を説明する他の図である。

図 15 は、図 1 の端末の動作を説明する他の図である。

図 16 は、パーソナルコンピュータの構成例を示すブロック図である。

発明を実施するための最良の形態

25 図 1 は、本発明を適用した端末 11 からなる情報通信システムの構成例を示している。

LAN 1-1, 1-2 (以下、個々に区別する必要がない場合、単位、LAN 1 と称

する。他の場合についても同様である）がインターネットに代表される WAN 2 を介して相互に接続されている。

LAN 1-1 は、例えば、家屋内に設けられ、特定の個人（あるいは、家族）が使用する程度の規模のものであり、それには、スイッチングハブ（図示せず）を介して、パーソナルコンピュータや A V 機器等の端末 1 1-1 および端末 1 1-2 が接続されている。LAN 1-1 と端末 1 1-1 および 1 1-2 との接続は、例えば、Ethernet（登録商標）（100BASE-TX）等の高速インタフェースによる。端末 1 1-1 および 1 1-2 は、LAN 1-1 および WAN 2 を介して、LAN 1-2 に接続することができる。

10 LAN 1-2 は、LAN 1-1 と同様に構成されており、それには、端末 1 1-3 が接続されている。

各端末 1 1 は、本情報通信システムに登録された正規の機器であり、図 2 に示すように、送信可否判定部 2 1、応答制御部 2 2、通信部 2 3、および送信データ格納部 2 4 を含んで構成されている。

15 送信可否判定部 2 1 は、他の端末 1 1（受信側の端末 1 1）に所定のデータを送信する際に、通信部 2 3 を介して、受信側の端末 1 1（正確には、その応答制御部 2 2）と後述するように通信することで、受信側の端末 1 1 が本情報通信システムにおける正規の機器であるか否かを認証するとともに、所定の要求に対する受信側の端末 1 1 の応答時間を、受信側の端末 1 1 との通信時間として計測する。

20 送信可否判定部 2 1 は、受信側の端末 1 1 の認証結果および応答時間に基づく通信距離の判別結果に基づいて、受信側の端末 1 1 に対するデータの送信可否を判定する。

例えば、受信側の端末 1 1 が、送信側の端末 1 1 と異なる LAN 1 に接続されている場合（WAN 2 を介して接続され、いわゆる通信距離が長い場合）、応答時間は、同じ LAN 1 に接続されている場合（通信距離が短い場合）に比べて長くなるので、例えば、通信が同一 LAN 1 内に制限されているとき、送信可否判定部 2 1 は、計

測した応答時間から受信側の端末 1 1 が送信側の端末 1 1 と同じ LAN 1 に接続されているか否かを判定し、その判定結果と受信側の端末 1 1 の認証結果に基づいて、データ送信の可否を判定する。

すなわち図 1 の例では、端末 1 1 - 1 (送信側) が端末 1 1 - 2 (受信側) に
5 データを送信する場合、端末 1 1 - 1 の送信可否判定部 2 1 は、計測した端末 1 1 - 2 の応答時間から、端末 1 1 - 2 が LAN 1 - 1 に接続されていることを判定し、データ送信を行う。一方、端末 1 1 - 1 が端末 1 1 - 3 にデータを送信する場合、端末 1 1 - 1 の送信可否判定部 2 1 は、計測した端末 1 1 - 3 の応答時間
10 から、端末 1 1 - 3 は LAN 1 - 1 と異なる LAN (LAN 1 - 2) に接続されていることを判定し、データ送信を行わない。

なおこのような通信距離による通信制御は、映画などのコンテンツを一定の地域に対して先行配給し、他の地域には後日配給するなどのコンテンツ配給ビジネスに適用することができる。

図 2 に戻り、応答制御部 2 2 は、送信側の端末 1 1 から所定のデータの送信を
15 受ける際、通信部 2 3 を介して、送信側の端末 1 1 (正確には、その送信可否判定部 2 1) と後述するように通信することで、送信側の端末 1 1 における認証および応答時間の適切な計測に必要な情報を送信側の端末 1 1 に送信する。

通信部 2 3 は、LAN 1 に接続されており、同一の LAN 1 内の端末 1 1、または WAN 2 を介して異なる LAN 1 に接続されている端末 1 1 との通信を行う。

20 送信データ格納部 2 4 は、受信側の端末 1 1 に送信される、所定のデータが格納されている。

図 3 は、端末 1 1 の送信可否判定部 2 1 の構成例を示している。

ランダムチャレンジ生成部 3 1 は、所定ビット数の疑似乱数 (以下、ランダム
25 チャレンジと称する) を生成し、ランダムチャレンジ送信制御部 3 2 および期待値生成部 3 3 に供給する。

ランダムチャレンジ送信制御部 3 2 は、ランダムチャレンジ生成部 3 1 から供給されたランダムチャレンジを、通信部 2 3 を介して、受信側の端末 1 1 に送信

する。ランダムチャレンジ送信制御部 3 2 はまた、通信部 2 3 を介して、受信側の端末 1 1 から送信されてきた、ランダムチャレンジを受信した旨のメッセージ（以下、RC受信メッセージと称する）を受信し、そのときRC受信メッセージを受信した旨をコマンド送信制御部 3 4 に通知する。

- 5 期待値生成部 3 3 は、ランダムチャレンジ生成部 3 1 から供給されたランダムチャレンジに対して、例えば、受信側の端末 1 1 と共有する秘密鍵を利用した HMAC (Keyed-Hashing for Message Authentication, IETF RFC 2104) アルゴリズムによるハッシュ処理（いわゆる鍵付きハッシュ処理）を施して、受信側の端末 1 1 でランダムチャレンジから生成される認証データの期待値を生成し、判定部 10 3 5 に供給する。期待値生成部 3 3 はまた、端末 1 1 に予め設定された端末 1 1 固有の情報（例えば、機器 ID）とランダムチャレンジを連結したものに鍵付きハッシュ処理を施して期待値を生成することもできる。

なお、ハッシュ処理で利用される秘密鍵は、本情報通信システムの正規の機器に所定のタイミングで安全に配信される。

- 15 コマンド送信制御部 3 4 は、ランダム送信制御部 3 2 から、RC受信メッセージを受信した旨が通知されたとき、または判定部 3 5 からの指示に従って、応答を要求するコマンド（以下、応答要求コマンドと称する）を、通信部 2 3 を介して、受信側の端末 1 1 に送信する。

- 20 コマンド送信制御部 3 4 または、通信部 2 3 を介して、送信した応答要求コマンドに対する応答として、受信側の端末 1 1 から送信されてきたメッセージ（以下、応答メッセージと称する）を受信し、それを判定部 3 5 に供給する。応答メッセージには、ランダムチャレンジ送信制御部 3 2 により送信されたランダムチャレンジから生成された認証データが組み込まれている。

- 25 コマンド送信制御部 3 4 または、応答要求コマンドを送信した後、応答時間計測部 3 6 を制御して、応答時間の計測を開始させるとともに、その応答要求コマンドに対する応答としての応答メッセージを受信したとき、応答時間の計測を終了させる。

判定部 3 5 は、コマンド送信制御部 3 4 からの応答メッセージに組み込まれている認証データと、期待値生成部 3 3 で生成されたその認証データの期待値に基づいて、受信側の端末 1 1 が、本情報通信システムにおける正規の機器であるかの認証を行う。判定部 3 5 はまた、応答時間計測部 3 6 で計測された応答時間が所定の時間 TL を越えているか否かを判定して、通信距離の判別（送信側の端末 1 1 と同一の LAN 1 に接続されているかの判定）を行う。

判定部 3 5 は、受信側の端末 1 1 の認証結果および通信距離の判別結果に基づいて、データの送信可否の判定を行う。判定部 3 5 は、その判定結果に基づいて、通信部 2 3 を制御し、送信データ格納部 2 4 に格納されているデータを、受信側の端末 1 1 に送信させる。

応答時間計測部 3 6 は、コマンド送信制御部 3 4 からの指示に従って、内蔵するタイマを動作させ、受信側の端末 1 1 の応答時間を計測する。

図 4 は、端末 1 1 の応答制御部 2 2 の構成例を示している。

ランダムチャレンジ受信制御部 4 1 は、通信部 2 3 を介して、送信側の端末 1 1（正確には、その送信可否判定部 2 1）から送信されてきたランダムチャレンジを受信し、それを認証データ生成部 4 2 に供給する。ランダムチャレンジ受信制御部 4 1 はまた、通信部 2 3 を介して、RC 受信メッセージ（ランダムチャレンジを受信した旨を表すメッセージ）を、送信側の端末 1 1 に送信し、そのとき RC 受信メッセージを送信した旨を応答メッセージ送信制御部 4 4 に通知する。

認証データ生成部 4 2 は、ランダムチャレンジ受信制御部 4 1 から供給されたランダムチャレンジに対して、送信側の端末 1 1（送信可否判定部 2 1 の期待値生成部 3 3）における場合と同様の鍵付きハッシュ処理を施して、第三者が予測できない認証データを生成し、応答メッセージ生成部 4 3 に供給する。

応答メッセージ生成部 4 3 は、応答メッセージ送信制御部 4 4 の制御に従って、認証データ生成部 4 2 から供給された認証データを組み込んだ応答メッセージを生成し、応答メッセージ送信制御部 4 4 に供給する。

応答メッセージ送信制御部 4 4 は、通信部 2 3 を介して、送信側の端末 1 1 か

ら送信されてきた応答要求コマンドを受信する。

応答メッセージ送信制御部 4 4 は、応答要求コマンドを受信する前のタイミングで（送信側の端末 1 1 から応答要求コマンドが送信されてくる前のタイミングで）、応答メッセージ生成部 4 3 を制御して、受信する応答要求コマンドに対応した認証データが組み込まれた応答メッセージを生成させるとともに、応答要求コマンドを受信したとき、通信部 2 3 を介して、その応答メッセージを送信先の端末 1 1 に送信する。

次に、図 5 のフローチャートを参照して、送信可否判定処理を行う場合の端末 1 1 の送信可否判定部 2 1（図 2， 3）の動作を説明する。

10 ステップ S 1 において、端末 1 1（送信側の端末 1 1）の送信可否判定部 2 1 のランダムチャレンジ生成部 3 1 は、ランダムチャレンジを生成し、それをランダムチャレンジ送信制御部 3 2 および期待値生成部 3 3 に供給する。

ステップ S 2 において、ランダムチャレンジ送信制御部 3 2 は、供給されたランダムチャレンジを、通信部 2 3 を介して受信側の端末 1 1 に送信し、ステップ
15 S 3 において、期待値生成部 3 3 は、供給されたランダムチャレンジに対して鍵付きハッシュ処理を施して、受信側の端末 1 1 で生成される認証データの期待値を生成する。

なおこの例の場合、送信側の端末 1 1 は、データ送信の可否を判定するのに、最大 N （ $= 1, 2, \dots$ ）回応答要求コマンドを送信するので、ここでは、送信
20 され得る N 個の応答要求コマンドに応じた認証データの N 個の期待値が生成される。

N 個の期待値は、例えば、ランダムチャレンジに対して鍵付きハッシュ処理を施した結果得られたデータを複数個に分割し、その分割して得られたデータから N 個の期待値を生成することができる。図 6 の例の場合、ランダムチャレンジに
25 対して鍵付きハッシュ処理を施した結果得られたデータが、 N 個に分割されて、 N 個の期待値 1 乃至期待値 N が生成される。

また、ランダムチャレンジに対する鍵付きハッシュ処理を、複数回繰り返して

行い、その処理毎に得られたデータから、N個の期待値を生成することができる。

図7の例の場合、ランダムチャレンジに対する鍵付きハッシュ処理がN回繰り返して行われ、その処理毎に得られたN個のデータが期待値となる。図7中、期待値1は、ランダムチャレンジに鍵付きハッシュ処理が1回施された結果得られたものであり、期待値2は、期待値1に、鍵付きハッシュ処理がさらに施された結果得られたものである。

図5に戻り、ステップS4において、ランダムチャレンジ送信制御部32は、後述するように受信側の端末11から送信されてきた、ステップS2で送信されたランダムチャレンジを受信した旨を示すRC受信メッセージを（ステップS2
10 3）、通信部23を介して受信し、その旨をコマンド送信制御部34に通知する。ステップS5において、コマンド送信制御部34は、応答要求コマンドが何番目に送信されるものか（送信の順番）を示すカウンタiに1を初期設定する。

次に、ステップS6において、コマンド送信制御部34は、通信部23を介して、応答要求コマンドを受信側の端末11に送信し、ステップS7において、応
15 答時間計測部36を制御して、応答時間の計測を開始させる。

ステップS8において、コマンド送信制御部34は、後述するように受信側の端末11から送信されてきた、ステップS6で送信された応答要求コマンドに対する応答しての応答メッセージを、通信部23を介して受信して、判定部35に供給し、ステップS9において、応答時間計測部36を制御して、応答時間の計
20 測を終了させる。すなわちステップS7で開始しステップS9で終了する時間計測で得られた時間が受信側の端末11の応答時間となる。

ステップS10において、判定部35は、コマンド送信制御部34から供給された応答メッセージに組み込まれている認証データと、期待値生成部33により生成された、その認証データの期待値（具体的には、カウンタiが示す順番に送信された応答要求コマンド（以下、第i番目に送信された応答要求コマンドと称
25 する）に対応する期待値）とが一致するか否かを判定し、一致すると判定した場合、受信側の端末11を、情報通信システムにおける正規の端末であると認証し、

ステップ S 1 1 に進む。

ステップ S 1 1 において、判定部 3 5 は、応答時間計測部 3 で計測された、第 i 番目に送信された応答要求コマンドに対する受信側の端末 1 1 の応答時間が所定の時間 TL を越えているか否かを判定する。時間 TL は、例えば、同一 LAN 1 に
5 接続された端末 1 1 間で要する通信時間である。すなわち応答時間が時間 TL を越える場合、受信側の端末 1 1 は、送信側の端末 1 1 と異なる LAN 1 に接続され、また、時間 TL を越えない場合（応答時間＝時間 TL を含む）、同一の LAN 1 に接続されていると判定することができる（通信距離を判別することができる）。

ステップ S 1 1 で、時間 TL を越えると判定された場合、ステップ S 1 2 に進み、
10 判定部 3 5 は、その結果を、コマンド送信制御部 3 4 に通知し、コマンド送信制御部 3 4 はそのとき、カウンタ i を 1 だけインクリメントする。

ステップ S 1 3 において、コマンド送信制御部 3 4 は、カウンタ $i = N + 1$ であるか否かを判定する。カウンタ $i = N + 1$ ではないと判定された場合には、所定時間経過後、ステップ S 6 に戻る。ステップ S 1 3 で、カウンタ $i = N + 1$ である
15 と判定されたとき（すなわち、応答要求コマンドの送信が N 回行われたとき）、またはステップ S 1 0 で、受信側の端末 1 1 が本情報通信システムにおける正規の機器ではないと判定されたとき、ステップ S 1 4 に進み、その旨を、判定部 3 5 に通知する。判定部 3 5 はそのとき、受信側の端末 1 1 へのデータ送信を不可とし、通信部 2 3 を制御して、送信データ格納部 2 4 に格納されているデータの
20 受信側の端末 1 1 に対する送信を禁止する。

ステップ S 1 1 で、第 i 番目に送信された応答要求コマンドに対する応答時間が、時間 TL を越えないと判定された場合、すなわち、受信側の端末 1 1 が、本情報通信システムにおける正規の機器であり、かつ、例えば送信側の端末 1 1 と同じ LAN 1 に接続されている端末 1 1 であるとき、ステップ S 1 5 に進み、判定部
25 3 5 は、通信部 2 3 を制御して、送信データ格納部 2 4 に格納されているデータを、受信側の端末 1 1 に送信させる。

ステップ S 1 4 またはステップ S 1 5 で、受信側の端末 1 1 に対するデータ送

信可否が判定されたとき、判定部 3 5 は、通信部 2 3 を介して、送信可否判定が終了した旨を表すメッセージ（以下、判定終了メッセージと称する）を受信側の端末 1 1 に送信する。その後、送信可否判定処理は、処理を終了する。

次に、図 5 のフローチャートを参照して、応答処理を行う場合の端末 1 1 の応答制御部 2 2（図 2， 4）の動作を説明する。

ステップ S 2 1 において、端末 1 1（受信側の端末 1 1）の応答制御部 2 2 のランダムチャレンジ受信制御部 4 1 は、送信先の端末 1 1 から送信されてきたランダムチャレンジを（ステップ S 2）、通信部 2 3 を介して受信し、認証データ生成部 4 2 に供給する。ステップ S 2 2 において、認証データ生成部 4 2 は、ランダムチャレンジ受信制御部 4 1 から供給されたランダムチャレンジに対して、送信側の端末 1 1 の送信可否判定部 2 1（期待値生成部 3 3）における鍵付きハッシュ処理（ステップ S 3）と同様の鍵付きハッシュ処理を施し、認証データを生成し、応答メッセージ生成部 4 3 に供給する。

なおこの例では、最大 N 個の応答要求コマンドを受信し得るので、その応答要求コマンドに対応する期待値と対比される（ステップ S 1 0）N 個の認証データが生成される。N 個の認証データは、期待値の生成方法（図 6， 7）と同じ方法で生成される。

このように認証データが生成されると、ステップ S 2 3 において、ランダムチャレンジ受信制御部 4 1 は、通信部 2 3 を介して、RC 受信メッセージを送信側の端末 1 1 に送信し、その旨を、応答メッセージ送信制御部 4 4 に通知する。

ステップ S 2 4 において、応答メッセージ送信制御部 4 4 は、これから受信する応答要求コマンドが何番目に受信されるものかを示すカウンタ j に 1 を初期設定し、ステップ S 2 5 において、応答メッセージ生成部 4 3 を制御して、カウンタ j が示す順番に受信される応答要求コマンド（以下、第 j 番目に受信される応答要求コマンドと称する）に対応する認証データを組み込んだ応答メッセージを生成させる。

次に、ステップ S 2 6 において、応答メッセージ送信制御部 4 4 は、送信先の

端末 1 1 から送信されてきた応答要求コマンドを (ステップ S 6)、通信部 2 3 を介して受信すると、ステップ S 2 7 において、ステップ S 2 5 で生成された第 j 番目に受信される応答要求コマンドに応じた認証データが組み込まれた応答メッセージを、通信部 2 3 を介して、送信側の端末 1 1 に送信する。これにより上述
5 したように送信側の端末 1 1 で (ステップ S 1 0 で)、第 j 番目に受信された (第 i 番目に送信された) 応答要求コマンドに対応する認証データと、第 i 番目に送信された (第 j 番目に受信された) 応答要求コマンドの期待値とが比較される。

ステップ S 2 8 において、受信側の端末 1 1 の応答制御部 2 2 の応答メッセージ送信制御部 4 4 は、送信側の端末 1 1 から送信される判定終了メッセージ (ステップ S 1 6) が受信されたか否かを判定し、所定の時間内に受信されていないと判定した場合、ステップ S 2 9 に進む。ステップ S 2 9 において、応答メッセージ送信制御部 4 4 は、カウンタ j を 1 だけインクリメントし、ステップ S 3 0
10 で、カウンタ $j = N + 1$ であるか否かを判定する。

ステップ S 3 0 で、カウンタ $j = N + 1$ ではないと判定されたとき (すなわち、
15 応答要求コマンドを N 回受信されていないとき)、ステップ S 2 5 に戻り、次に受信される応答要求コマンドに対して、それ以降の処理を実行する。

ステップ S 2 8 で、判定終了メッセージが受信されたとき、またはステップ S 3 0 で、カウンタ $j = N + 1$ であると判定されたとき (すなわち、応答要求コマンドが N 回受信されたとき)、応答制御部 2 2 は、応答処理を終了する。

20 以上のように、ランダムチャレンジから生成された認証データ (ステップ S 2 2) とその期待値 (ステップ S 3) とに基づいて認証された受信側の端末 1 1 についてのみ応答時間に基づく通信距離の判別を行うようにしたので (ステップ S 1 0 で NO の判定がなされた場合、ステップ S 1 1 の処理がスキップされるので)、正規の機器のようになりすました機器にデータが送信されることを防止することが
25 できる (正規の機器のようになりすました機器が応答要求コマンドを受信し、応答要求メッセージを送信して、その機器にデータが送信されることはない)。

また送信側の端末 1 1 で、応答要求コマンドに、新たに生成したランダムチャ

レンジを組み込んで受信側の端末 1 1 に送信し (ステップ S 6)、受信側の端末 1 1 で、応答要求コマンドを受信したとき (ステップ S 2 6)、予め生成された認証データ (ステップ S 2 2) と、その応答要求コマンドに組み込まれたランダムチャレンジとを連結して、または両者の論理演算を行って新たな認証データを生成し、それを組み込んだ応答メッセージを返信することもできる (ステップ S 2 7)。なおこのとき送信側の端末 1 1 では、ステップ S 1 0 で新たな認証データと比較される期待値が、ステップ S 3 で生成された期待値と、応答要求コマンドに組み込まれたランダムチャレンジと連結されて、または両者の論理演算が行われて生成される。

- 10 このように応答要求コマンドに組み込んだランダムチャレンジを利用して認証データおよび期待値が生成されるようにすることで、受信側の端末 1 1 は、送信側の端末 1 1 からの応答要求コマンドを受信した後でなければ、応答メッセージを送信することができなくなる。したがって、応答時間を短縮するために、応答要求コマンドを受信する前に応答メッセージを送信するなどといった不正行為を
- 15 防止することができる。

また、以上のように、受信側の端末 1 1 において、応答要求コマンドを受信する前に、認証データおよびそれが組み込まれた応答メッセージを生成するようにしたので (ステップ S 2 2, S 2 5)、応答要求コマンドを受信した後直ちに応答メッセージを送信側の端末 1 1 に返信することができる (ステップ S 2 7)。

- 20 例えば、応答要求コマンドを受信した後に、認証データおよび応答要求メッセージを生成するようになされている場合、送信側の端末 1 1 で計測される応答時間に、その処理にかかる時間が含まれてしまうので、通信時間としての応答時間を正確に計測することができない。しかしながら本発明のように応答要求コマンドを受信した後直ちに応答メッセージを送信することができるようにしておくことにより、通信時間としての応答時間が正確に計測される。
- 25

また、以上においては、送信側の端末 1 1 がランダムチャレンジを生成し (ステップ S 1)、受信側の端末 1 1 に提供するようにしたが (ステップ S 2)、受信

側の端末 1 1 が生成して送信側の端末 1 1 に提供するようにすることもできる。

また、以上においては、秘密鍵を送信側の端末 1 1 と受信側の端末 1 1 で共有している場合を例として説明したが、秘密鍵の共有がない場合には、デフィー・ヘルマン鍵交換 (Diffie-Hellman key exchange) のアルゴリズムなどを使って鍵の共有を行うことができる。この場合は、鍵交換した相手は、応答時間を測定する相手であることの証明書などを基に確認される。鍵交換の後、鍵交換で得られた鍵そのものを認証データと期待値とすることもできるし、上記のように乱数に交換した鍵での鍵付きハッシュ処理を施し、認証データや期待値を得るようにすることもできる。

- 10 また以上においては、送信側の端末 1 1 において、受信側の端末 1 1 で生成された応答の認証データ (以下、認証データ RR と称する) (ステップ S 2 2) と送信側の端末 1 1 で生成された応答の期待値 (以下、期待値 QR と称する) (ステップ S 3) とに基づき受信側の端末 1 1 が認証されたが (ステップ S 1 0)、受信側の端末 1 1 においても、送信側の端末 1 1 からの応答要求コマンドの認証データ
- 15 (以下、認証データ RS と称する) とその期待値 (以下、期待値 QS と称する) とに基づき送信側の端末 1 1 の認証を行うようにすることができる。

- 図 5 の例では、受信側の端末 1 1 は、応答要求コマンドを受ければ (ステップ S 2 6)、直ちに応答メッセージを送り返すので (ステップ S 2 7)、例えば、図 8 に示すように、送信側の端末 1 1 (送信機器) と同一の LAN 1 に第 3 の機器 x
- 20 を挿入し、はじめに機器 x が受信機器に応答要求コマンドを送って (S 1 1 1)、受信機器から応答メッセージを取得しておき (S 1 1 2)、そして送信機器から応答要求コマンドが来たときに (S 1 2 1)、取得した応答メッセージを返すことで (S 1 2 2)、機器 x は、正規の機器になりすますことができる。

- そこで受信側の端末 1 1 においても、応答メッセージを返信する際に、送信側の
- 25 端末 1 1 を認証すれば、このような不正を防止することができる (不正な機器に応答メッセージを返信することを防止することができる)。

図 9 は、送信可否判定部 2 1 の、図 1 0 は、応答制御部 2 2 の、このように受

信側の端末 1 1 でも送信側の端末 1 1 の認証がなされる場合の構成例を示している。

送信可否判定部 2 1 のランダムチャレンジ生成部 5 1 は、図 3 のランダムチャレンジ生成部 3 1 と同様に、所定ビット数の疑似乱数列を、ランダムチャレンジ RC として生成し、期待値生成部 5 2 および認証データ生成部 5 3 に供給する。

期待値生成部 5 2 は、ランダムチャレンジ生成部 5 1 から供給されたランダムチャレンジ RC に対して、例えば、受信側の端末 1 1 と共有する秘密鍵を利用した受信側の端末 1 1（認証データ生成部 7 3）における場合と同様の鍵付きハッシュ処理を施して、受信側の端末 1 1 の認証データ RR の期待値 QR（対応する認証データ RR と同値の期待値 QR）を生成し、応答認証部 5 7 に供給する。

認証データ生成部 5 3 は、ランダムチャレンジ生成部 5 1 から供給されたランダムチャレンジ RC に対して、受信側の端末 1 1 と共有する秘密鍵を利用した鍵付きハッシュ処理を施して、第三者が予測できないコマンドの認証データ RS を生成し、応答要求コマンド送信部 5 5 に供給する。

制御コマンド通信制御部 5 4 は、開始コマンド等の制御コマンド CC を受信側の端末 1 1 に送信したり、受信側の端末 1 1 から送信されてきた、制御コマンド CC に対する応答メッセージ CCR を受信する。

応答要求コマンド送信部 5 5 は、認証データ生成部 5 3 により生成された認証データ RS を含む、応答要求コマンド MC を、通信部 2 3 を介して、受信側の端末 1 1 に送信する。

応答受信部 5 6 は、送信された応答要求コマンド MC に対する応答として、受信側の端末 1 1 から送信されてきた応答メッセージ MCR を、通信部 2 3 を介して受信し、そこに組み込まれている応答の認証データ RR を応答認証部 5 7 に供給する。

応答認証部 5 7 は、応答受信部 5 6 からの応答の認証データ RR と、期待値生成部 5 2 で生成されたその認証データ RR の期待値 QR に基づいて、受信側の端末 1 1 が、本情報通信システムにおける正規の機器であるかの認証を行い、その認証結果を、制御判定部 5 8 に通知する。

制御判定部 5 8 は、応答時間計測部 5 9 で計測された、応答要求コマンド MC に対する受信側の端末 1 1 の応答時間 RTT が所定の時間 TL を越えているか否かを判定して、通信距離の判別（送信側の端末 1 1 と同一の LAN 1 に接続されているかの判定）を行う。

- 5 制御判定部 5 8 は、受信側の端末 1 1 の認証結果および通信距離の判別結果に基づいて、受信側の端末 1 1 に対するデータの送信可否の判定を行う。制御判定部 5 8 は、その判定結果に基づいて、通信部 2 3 を制御し、送信データ格納部 2 4 に格納されているデータを、受信側の端末 1 1 に送信させる。

- 10 応答時間計測部 5 9 は、応答要求コマンド送信部 5 5 および応答受信部 5 6 からの通知に応じて、応答要求コマンド MC に対する、受信側の端末 1 1 の応答時間 RTT を計測する。

次に、応答制御部 2 2 の構成（図 1 0）を説明する。

- 15 制御応答通信制御部 7 1 は、通信部 2 3 を介して、送信側の端末 1 1 から送信されてきた制御コマンド CC を受信したり、その制御コマンド CC に対する応答メッセージ CCR を送信側の端末 1 1 に送信する。

- 20 期待値生成部 7 2 は、制御応答通信制御部 7 1 により受信された制御コマンド CC に含まれるランダムチャレンジ RC に対して、送信側の端末 1 1 と共有する秘密鍵を利用した送信側の端末 1 1（認証データ生成部 5 3）における場合と同様の鍵付きハッシュ処理を施して、送信側の端末 1 1 のコマンド認証データ RS の期待値 QS（対応する認証データ RS と同値の期待値 QS）を生成し、コマンド認証部 7 6 に供給する。

- 25 認証データ生成部 7 3 は、制御応答通信制御部 7 1 により受信された制御コマンド CC に含まれるランダムチャレンジ RC に対して、送信側の端末 1 1 と共有する秘密鍵を利用した鍵付きハッシュ処理を施して、第三者が予測できない応答の認証データ RR を生成し、応答送信部 7 4 に供給する。

応答送信部 7 4 は、コマンド認証部 7 6 による認証結果に基づいて、認証データ生成部 7 3 により生成された応答の認証データ RR を含む、送信側の端末 1 1 か

らの応答要求コマンド MC に対する応答メッセージ MCR を、通信部 2 3 を介して送信側の端末 1 1 に送信する。

5 応答要求コマンド受信部 7 5 は、送信側の端末 1 1 から送信されてきた応答要求コマンド MC を、通信部 2 3 を介して受信し、そこに組み込まれているコマンドの認証データ RS をコマンド認証部 7 6 に供給する。

コマンド認証部 7 6 は、応答要求コマンド受信部 7 5 からのコマンドの認証データ RS と、期待値生成部 7 2 で生成されたその認証データ RS の期待値 QS に基づいて、送信側の端末 1 1 が、本情報通信システムにおける正規の機器であるかの認証を行い、その認証結果を、応答送信部 7 4 に通知する。

10 次に、図 9 の送信可否判定部 2 1 の動作を、図 1 1 のフローチャートを参照して説明する。

ステップ S 5 1 において、端末 1 1 の送信可否判定部 2 1 の制御コマンド通信制御部 5 4 は、受信側の機器と、TCP コネクションを確立する。TCP コネクションのためのポート番号は予め送信側の端末 1 1 と受信側の機器の間で合意されているものとする。送信側の機器と受信側の機器の間で事前に TCP コネクションが確立している場合はこのステップを省略してよい。

制御コマンド通信制御部 5 4 は、確立した TCP コネクションを介して、応答時間 RTT の計測を開始する旨を表す開始コマンド（制御コマンド CC）を受信側の機器に送信する。この開始コマンド CC には、セッション番号 SID、ランダムチャレンジ RC、送信側の端末 1 1 が実行可能な、1 セッションでの応答時間 RTT の計測のリトライ数（計測回数）ks が含まれている。

セッション番号 SID は、これから行われる受信側の機器に対する一連の認証処理（1 つのセッション）に割り当てられた番号であり、この番号を送信側と受信側とで共有することにより、セッション毎に認証処理を区別することができる。

25 また応答時間 RTT の計測のために必要なデータ（例えば、応答要求コマンド MC やその応答メッセージ MCR）の通信は、パケットの再送を行わない UDP でなされるので、通信状態によっては、データが途中で消滅してしまうなど、応答時間 RTT

の計測が適切に行われない場合も考えられる。またネットワーク内の他の通信の影響を受けて、パケットの伝送に遅延が生じることもある。そこで応答時間 RTT の計測を何回かリトライ（再施行）できるようになされている。このリトライの回数は、送信側の機器と受信側の機器の設定によって異なることもあるので、この例ではここで送信側の機器のリトライ数（例えば、最大のリトライ数） k_s が受信側の機器に通知される。

次に、ステップ S 5 2 において、制御コマンド通信制御部 5 4 は、開始コマンド CC に対する、受信側の機器からの応答メッセージ CCR を受信する。

この応答メッセージ CCR には、開始コマンド CC に含まれていたセッション番号 SID の他、受信側が決定した 1 セッションでの応答時間 RTT 計測のリトライ数 k 、および応答要求コマンド MC を受信するための UDP ポート番号 p_b が含まれている。すなわち開始コマンド CC とその応答メッセージ CCR の授受により、送信側の端末 1 1 と受信側の機器は、応答時間 RTT の計測のリトライ数（計測回数） k とセッション番号 SID、および応答要求コマンド MC とその応答メッセージ MCR の授受のために利用する UDP ポート番号 p_b を合意する。

なお受信側の機器は、開始コマンド CC を介して通知された送信側の端末 1 1 で実行可能な応答時間 RTT 計測のリトライ数 k_s と受信側が実行可能な応答時間 RTT 計測のリトライ数のうちの小さい方を、今回の応答時間 RTT 計測のリトライ数 k に決定し、応答メッセージ CCR を介して送信側の機器に通知する。

ステップ S 5 3 において、期待値生成部 5 2 は、ランダムチャレンジ生成部 5 1 により生成されたランダムチャレンジ RC に対して、受信側の端末 1 1 の応答制御部 2 2（認証データ生成部 7 3）における鍵付きハッシュ処理と同様の鍵付きハッシュ処理を施し、受信側の機器の認証データ RR の期待値 QR を生成する。

この例の場合、応答時間 RTT 計測が最大 k 回行われるので（応答要求コマンド MC の応答メッセージ MCR が最大 k 回受信されるので）、受信され得る k 個の応答メッセージ MCR に含まれる認証データ RR それぞれの期待値 QR が生成される。

またこのとき認証データ生成部 5 3 は、ランダムチャレンジ生成部 5 1 により

生成されたランダムチャレンジ RC に対して鍵付きハッシュ処理を施して、コマンドの認証データ RS を生成する。

この例の場合、応答時間 RTT 計測が最大 k 回行われるので（応答要求コマンド MC が最大 k 回送信されるので）、送信され得る k 個の応答要求コマンド MC それぞれの認証データ RS が生成される。

ステップ S 5 4 において、制御判定部 5 8 に内蔵されるカウンタ i の値が 1 に初期設定される。このとき期待値生成部 5 2 は、カウンタ i の値に対応する期待値 QR（例えば、第 i 番目に生成された期待値 QR_i）を応答認証部 5 7 に供給する。また認証データ生成部 5 3 は、カウンタ i の値に対応する認証データ RS_i を、応答要求コマンド送信部 5 5 に供給する。

ステップ S 5 5 において、応答要求コマンド送信部 5 5 は、セッション番号 SID、認証データ生成部 5 3 から供給された認証データ RS_i（k 個の認証データ RS のうちのカウンタ i の値に対応する認証データ RS_i）、およびシーケンス番号 C_i（カウンタ i の値を表す番号）を含む応答要求コマンド MC を、制御コマンド CC の応答 CCR に含まれていた UDP ポート番号 pb での UDP 通信で、受信側の機器に送信する。

応答要求コマンド送信部 5 5 は、応答要求コマンド MC を送信したとき、その旨の通知 STR を応答時間計測部 5 9 に行う。これにより応答時間計測部 5 9 は、応答時間の計測を開始する。

ステップ S 5 6 において、応答受信部 5 6 は、受信側の機器からの応答メッセージ MCR を受信したか否かを判定し、受信していないと判定した場合、ステップ S 5 7 に進み、所定時間以上応答を待っているか否かを判定する（ステップ S 5 5 で応答時間 RTT 計測が開始されてから所定の時間経過したか否かを判定する）。

ステップ S 5 7 で、まだ所定の時間経過していないと判定された場合、ステップ S 5 6 に戻り、それ以降の処理が実行される。一方ステップ S 5 7 で所定の時間経過したと判定された場合、ステップ S 6 2 に進み、カウンタ i の値がリトライ数 k より小さいか否かが判定され（応答時間 RTT の計測が k 回行われたか否かが判定され）、小さいと判定された場合（k 回行われていない場合）、ステップ S

6 3に進み、カウンタ i の値が 1 だけインクリメントされて、ステップ S 5 5 に戻る。

応答要求コマンド MC を送る UDP では、パケットが通信相手に届かないことがあるので、送信側の端末 1 1 は、応答要求コマンド MC を送った後、所定時間が経っても応答メッセージ MCR が受信されない場合は、この回の計測は失敗したものとして、次の応答時間 RTT の計測が開始される（ステップ S 5 5 以降の処理が開始される）。

ステップ S 5 6 で、応答メッセージ MCR が受信されたと判定された場合、ステップ S 5 8 に進み、応答受信部 5 6 は、受信した応答メッセージ MCR に含まれている応答の認証データ RR_j 、およびシーケンス番号 C_j を読み出し、応答認証部 5 7 に供給する。

応答認証部 5 7 は、応答受信部 5 6 から供給されたシーケンス番号 C_j が、カウンタ i の値（送信された応答要求コマンド MC のシーケンス番号 C_i ）と一致するか否かを判定する。

15 なお応答メッセージ MCR のシーケンス番号 C_j と応答要求コマンド MC のシーケンス番号 C_i を確認することの効果については後述する。

ステップ S 5 8 で、一致しないと判定された場合、ステップ S 5 6 に戻り、それ以降の処理が行われ、一致すると判定された場合、ステップ S 5 9 に進む。

20 ステップ S 5 9 において、応答受信部 5 6 は、応答メッセージ MCR を受信した旨の通知 END を応答時間計測部 5 9 に行う。応答時間計測部 5 9 は、ステップ S 5 5 で開始した応答時間 RTT 計測を終了し、計測結果（応答時間 RTT）を、制御判定部 5 8 に供給する。

25 ステップ S 6 0 において、応答認証部 5 7 は、応答受信部 5 6 から供給された応答の認証データ RR_j と、期待値生成部 5 2 により生成された、その認証データ RR_j の期待値 QR_i とが一致するか否かを判定し、一致すると判定した場合、受信側の端末 1 1 を、本情報通信システムにおける正規の端末であると認証し、ステップ S 6 1 に進む。

ステップ S 6 1 において、制御判定部 5 8 は、応答時間計測部 5 9 から供給された応答時間 RTT が、所定の規定時間 TL より大きいかな否かを判定する。

規定時間 TL は、応答時間 RTT が、送信側の端末 1 1 と受信側の機器が同一 LAN 1 に接続されていたならば、それを超えないであろう時間である。すなわち応答時間 RTT が規定時間 TL より大きければ、受信側の機器は送信側の端末 1 1 と同一の LAN 1 に接続されていないと判定することができる。一方、応答時間 RTT が規定時間 TL より大きくない（それ以下である場合）、受信側の機器は送信側の端末 1 1 と同一 LAN 1 に接続されていると判定することができる。

ステップ S 6 1 で、YES の判定がなされたとき（第 i 回目の応答時間 RTT 計測で、受信側の機器が送信側の端末 1 1 と同一の LAN 1 に接続されているものではないと判定されたとき）、ステップ S 6 2 に進み、制御判定部 5 8 は、カウンタ i の値が k より小さい値かな否か（応答時間 RTT 計測が k 回リトライされたかな否か）を判定し、小さいと判定した場合（応答時間 RTT 計測がまだ k 回行われていない場合）、ステップ S 6 3 に進み、カウンタ i の値が 1 だけインクリメントされる。このとき期待値生成部 5 2 は、カウンタ i の新たな値に対応する期待値 QRi を応答認証部 5 7 に供給し、認証データ生成部 5 3 は、カウンタ i の新たな値に対応する認証データ RSi を、応答要求コマンド送信部 5 5 に供給する。

その後ステップ S 5 5 に戻り、それ以降の処理が行われる。すなわち応答時間 RTT が規定時間 TL 内になる応答メッセージ MCR が得られるまで、最大 k 回、応答時間 RTT の計測が行われる。

ステップ S 6 1 で、NO の判定がなされたとき（応答時間 RTT が規定時間 TL 以下となる応答メッセージ MCR が得られたとき）、ステップ S 6 4 に進む。

ステップ S 6 4 に進み、制御判定部 5 8 は、受信側の機器は、送信データを送信できる機器（正規の機器であって、送信側の端末 1 1 と同じ LAN 1 に接続されている機器）である旨を、通信部 2 3（図 3）に通知する。これにより通信部 2 3 は、所定の送信データを送信データ格納部 2 4 から読み出して、受信側の機器（端末 1 1）に送信する。

ステップ S 6 2 で、カウンタ i の値が、 k 以上であると判定された場合（応答時間 RTT の計測を k 回行っても、応答時間 RTT が規定時間 TL 以下になる応答が得られなかった場合）、ステップ S 6 5 に進み、制御判定部 5 8 は、受信側の機器は、ローカルネットワーク外の機器（送信側の端末 1 1 と同じ LAN 1 に接続されていない機器）である旨を、制御コマンド通信制御部 5 4 に通知する。これにより制御コマンド通信制御部 5 4 は、受信側の機器の認証が失敗した旨を示す終了コマンド CC を、受信側の機器に送信する。

ステップ S 6 0 で、応答の認証データ RR_j とその期待値 QR_i 一致しないと判定された場合、ステップ S 6 6 に進み、制御判定部 5 8 は、受信側の機器は、不正な機器である旨を、制御コマンド通信制御部 5 4 に通知する。これにより制御コマンド通信制御部 5 4 は、受信側の機器の認証が失敗した旨を示す終了コマンド CC を、受信側の機器に送信する。

以上のようにして送信可否判定処理が行われる。

なお以上においては、ステップ S 5 3 において k 個の認証データ RS を生成したが、それに代えて、ステップ S 5 5 において、応答要求コマンド MC を送信する毎にそのコマンドに使う認証データ RS を毎回生成するようにしてもよい。

次に、図 1 0 の応答制御部 2 2 の動作を、図 1 2 のフローチャートを参照して説明する。

ステップ S 8 1 において、受信側の端末 1 1 の応答制御部 2 2 の制御応答通信制御部 7 1 は、送信側の機器と協働して、TCP コネクションを確立し、その TCP コネクションを介して送信側の機器から送信されてきた、開始コマンド CC（ステップ S 5 1）を受信する。制御応答通信制御部 7 1 は、受信した開始コマンド CC に含まれているランダムチャレンジ RC を、期待値生成部 7 2 および認証データ生成部 7 3 に供給する。

次にステップ S 8 2 において、応答要求コマンド受信部 7 5 は、送信側の機器から送信されてくる応答要求コマンド MC を受信するための UDP ポート番号 pb を決定する。

応答要求コマンド受信部 7 5 はまた、制御コマンド CC に含まれている送信側の機器が実行可能な応答時間 RTT 計測のリトライ数 k_s と、受信側の端末 1 1 が対応可能な応答時間 RTT の計測のリトライ数のいずれか小さい方を、今回の応答時間 RTT の計測のリトライ数 k に決定する。

5 ステップ S 8 3 において、制御応答通信制御部 7 1 は、ステップ S 8 1 で受信された制御コマンド CC に含まれていたセッション番号 SID、応答時間 RTT の計測のリトライ数 k 、および UDP ポート番号 pb を含む応答メッセージ CCR を、ステップ S 8 1 で確立された TCP コネクトを介して送信側の機器に送信する。送信側の機器は、ここで送信された応答メッセージ CCR を受信する（ステップ S 5 2）。

10 ステップ S 8 4 において、認証データ生成部 7 3 は、制御応答通信制御部 7 1 から供給されたランダムチャレンジ RC に対して鍵付きハッシュ処理を施して、応答の認証データ RR を生成する。

この例の場合、応答時間 RTT 計測が最大 k 回行われるので（応答要求コマンド MC の応答メッセージ MCR が最大 k 回送信されるので）、送信され得る k 個の応答
15 メッセージ MCR それぞれの認証データ RR が生成される。

期待値生成部 7 2 は、制御応答通信制御部 7 1 から供給されたランダムチャレンジ RC に対して、送信側の端末 1 1 の送信可否判定部 2 1（認証データ生成部 5 3）における鍵付きハッシュ処理と同様の鍵付きハッシュ処理を施し、送信側の端末 1 1 の認証データ RS の期待値 QS を生成する。

20 この例の場合、応答時間 RTT 計測が最大 k 回行われるので（応答要求コマンド MC が最大 k 回受信されるので）、受信され得る k 個の応答要求コマンド MC に含まれる認証データ RS それぞれの期待値 QS が生成される。

ステップ S 8 5 において、コマンド認証部 7 6 に内蔵されているカウンタ j の値が 1 に初期設定される。

25 ステップ S 8 6 において、コマンドが受信されるまで待機され、コマンドが受信されたと判定された場合、ステップ S 8 7 に進み、受信されたコマンドが応答要求コマンド MC（ステップ S 5 5）であるか否かを判定し、応答要求コマンド MC

であると判定された場合、ステップ S 8 8 に進む。

ステップ S 8 8 において、受信されたコマンドに含まれるシーケンス番号 C_i とカウンタ j が比較され、シーケンス番号 C_i がカウンタ j 以上の値であることが確認される。カウンタ j 以上の値である場合、ステップ S 8 9 に進み、カウンタ j がシーケンス番号 C_i の値に設定される。

これは、コマンドが欠落した場合、順番どおりに来なかった場合に、カウンタ j をシーケンス番号 C_i に合致させるための対策である。

期待値生成部 7 2 はこのとき、カウンタ j の値に対応する期待値 QS （例えば、第 j 番目に生成された期待値 QS_j ）をコマンド認証部 7 6 に供給する。また認証データ生成部 7 3 は、カウンタ j の値に対応する認証データ RR_j を、応答送信部 7 4 に供給する。

次にステップ S 9 0 において、コマンド認証部 7 6 は、応答要求コマンド受信部 7 5 により受信された応答要求コマンド MC に組み込まれている認証データ RS_i と、期待値生成部 7 2 により生成された期待値 QS_j （カウンタ j が示す順番に生成された期待値）とが一致するか否かを判定し、一致すると判定した場合、送信側の端末 1 1 を、本情報通信システムにおける正規の端末であると認証し、ステップ S 9 1 に進む。

ステップ S 9 1 において、コマンド認証部 7 6 は、送信側の端末 1 1 が正規の機器である旨を、応答送信部 7 4 に通知する。これにより応答送信部 7 4 は、セッション番号 SID 、カウンタ j の値を表すシーケンス番号 C_j 、認証データ生成部 7 3 から供給された認証データ RR_j を含む応答メッセージ MCR を、送信側の機器に送信する。

一方ステップ S 9 0 で、一致しないと判定された場合、ステップ S 9 2 に進み、コマンド認証部 7 6 は、その旨を、応答送信部 7 4 に通知する。これにより応答送信部 7 4 は、セッション番号 SID 、カウンタ j の値を表すシーケンス番号 C_j 、および送信側の機器における受信側の機器の認証（ステップ S 6 0）が失敗するような認証データ $RR (= \times \times)$ を含む応答メッセージ MCR を、送信側の機器に送

信する。

ステップ S 9 1 またはステップ S 9 2 で、応答メッセージ MCR が送信されたとき、ステップ S 9 3 で、カウンタ j の値が 1 だけインクリメントされ、その後、ステップ S 8 6 に戻り、それ以降の処理が実行される。

- 5 また、ステップ S 8 8 において、カウンタ j の値が受信されたコマンドに含まれるシーケンス番号 C_i よりも小さい場合も、ステップ S 8 6 に戻り、それ以降の処理が実行される。

10 ステップ S 8 7 で、受信されたコマンドが応答要求コマンドではないと判定された場合（終了コマンド CC（ステップ S 6 5, S 6 6）であるとき）、処理は終了する。

次に図 1 1 のステップ S 5 8 の処理について説明する。ステップ S 5 8 の処理では、受信側の機器からの応答メッセージ MCR のシーケンス番号 C_j と応答要求コマンド MC のシーケンス番号 C_i （カウンタ i の値）が一致するか否かが判定されるが、このように応答要求コマンド MC と応答メッセージ MCR の対応関係を確認するようにしたので、応答要求コマンド MC に対応しない応答メッセージ MCR（他の
15 応答要求コマンド MC の応答メッセージ MCR）に基づいて応答時間 RTT による距離判定が行われない。

例えば、図 1 3 に示すように、受信側の機器で、第 1 番目の応答要求コマンド MC に対する応答メッセージ MCR の送信に時間がかかり（ステップ S 9 1, S 9 2）、
20 送信側の端末 1 1 で、タイムアウトと判定されて（ステップ S 5 7）、第 2 番目の応答要求コマンド MC が受信側の機器に送信されたものとする。第 1 番目の応答要求コマンド MC に対する応答メッセージ MCR は、第 2 番目の応答要求コマンド MC が送信された後（ステップ S 5 5）、第 2 番目の応答要求コマンド MC との関係でタイムアウトとならない間（ステップ S 5 7）に送信側の端末 1 1 に受信された
25 ものとする（ステップ S 5 6）。

しかしながらこの場合本発明では、受信側の機器からの第 1 番目の応答メッセージ MCR のシーケンス番号（= 1）と、第 2 番目の応答要求コマンド MC のシーケ

ンス番号 (= 2) が一致しないと判定され、送信側の端末 1 1 は、第 2 番目の応答要求コマンド MC に対する応答メッセージ MCR が受信されるまで待機することになり (ステップ S 5 6 に戻る)、対応しない応答メッセージ MCR が受信されても応答時間 RTT による距離判定は行われない。

5 次に、不正に対する端末 1 1 の動作を具体的に説明する。

例えば図 8 に示した送信機器と同一の LAN 1 に接続された不正な機器 x が、受信機器から応答を得るために応答要求コマンドを送信するものとする。しかしながら、機器 x は、受信機器と共有する秘密鍵を有していないので、受信機器での送信機器の認証に必要な認証データ RS を得ることができない。したがって図 1 4
10 に示すように、機器 x が、不適当な認証データ RS (= ?) を含む応答要求コマンド MC を受信機器に送信するが、受信機器からは、受信機器の認証が失敗する認証データ RR (= × ×) を含む応答メッセージ MCR が送信されてくる (ステップ S 9 2)。したがって機器 x が、その後、送信機器からの応答要求コマンド MC に対して、その応答メッセージ MCR を送信機器に送信して応答しても、送信機器において、機器 x は認証されず、送信データは機器 x に送信されない。
15

そこで図 1 5 に示すように、不正の機器 x は、送信機器から応答要求コマンド MC を受けてそれを受信機器に送信し、受信機器から、適当な認証データ RR を含む応答メッセージ MCR を取得する。そして機器 x は、取得した応答メッセージ MCR を、送信機器に送信することもある。

20 しかしながらこの例の場合、応答要求コマンド MC は、送信機器から機器 x、そして機器 x から受信機器に送信され、応答メッセージ MCR が、受信機器から機器 x に、そして機器 x から送信機器へ伝送されるので、応答要求コマンド MC と応答メッセージ MCR の伝送路が、通常の伝送経路 (送信機器と受信機器間の伝送路) より長くなる。したがってこの場合、結局応答時間 RTT が規定時間 TL より長くなるので、機器 x は、送信機器と同一 LAN 1 に接続されていないものとして、機器
25 x には送信データが提供されない。

上述した一連の処理は、ハードウェアにより実現させることもできるが、ソフ

トウェアにより実現させることもできる。一連の処理をソフトウェアにより実現する場合には、そのソフトウェアを構成するプログラムがコンピュータにインストールされ、そのプログラムがコンピュータで実行されることより、上述した送信可否判定部 2 1 および応答制御部 2 2 が機能的に実現される。

- 5 図 1 6 は、上述のような送信可否判定部 2 1 および応答制御部 2 2 として機能するコンピュータ 1 0 1 の一実施の形態の構成を示すブロック図である。CPU (Central Processing Unit) 1 1 1 にはバス 1 1 5 を介して入出力インタフェース 1 1 6 が接続されており、CPU 1 1 1 は、入出力インタフェース 1 1 6 を介して、ユーザから、キーボード、マウスなどよりなる入力部 1 1 7 から指令が入力され
- 10 ると、例えば、ROM (Read Only Memory) 1 1 2、ハードディスク 1 1 4、またはドライブ 1 2 0 に装着される磁気ディスク 1 3 1、光ディスク 1 3 2、光磁気ディスク 1 3 3、若しくは半導体メモリ 1 3 4 などの記録媒体に格納されているプログラムを、RAM (Random Access Memory) 1 1 3 にロードして実行する。これにより、上述した各種の処理が行われる。さらに、CPU 1 1 1 は、その処理結果を、
- 15 例えば、入出力インタフェース 1 1 6 を介して、LCD (Liquid Crystal Display) などよりなる出力部 1 1 8 に必要に応じて出力する。なお、プログラムは、ハードディスク 1 1 4 や ROM 1 1 2 に予め記憶しておき、コンピュータ 1 0 1 と一体的にユーザに提供したり、磁気ディスク 1 3 1、光ディスク 1 3 2、光磁気ディスク 1 3 3、半導体メモリ 1 3 4 等のパッケージメディアとして提供したり、衛
- 20 星、ネットワーク等から通信部 1 1 9 を介してハードディスク 1 1 4 に提供することができる。

なお、本明細書において、記録媒体により提供されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

産業上の利用可能性

第 1 および第 3 の本発明によれば、受信装置の応答時間を適切に計測することができる。

- 5 第 2 および第 4 の本発明によれば、送信装置における応答時間の適切な計測に必要な情報を提供することができる。

請求の範囲

1. 受信装置との間で共有する共有データに基づいて認証データが生成された後、応答を要求するコマンドを前記受信装置に送信するコマンド送信手段と、
前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づいて前記受信装置を認証する認証手段と、
5 前記受信装置からの、前記コマンドに対する応答時間を計測する計測手段と、
前記認証手段による認証結果、および前記計測手段により計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定手段と
を備えることを特徴とする情報処理装置。
- 10 2. 前記コマンド送信手段は、データの送信可否を判定するのに、前記コマンドを最大N回送信し、
前記認証手段は、前記コマンドの送信の順番に応じた前記認証データとその前記期待値とに基づいて、前記受信装置を認証する
ことを特徴とする請求の範囲第1項に記載の情報処理装置。
- 15 3. 受信装置との間で共有する共有データに基づいて認証データが生成された後、応答を要求するコマンドを前記受信装置に送信するコマンド送信ステップと、
前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づいて前記受信装置を認証する認証ステップと、
前記受信装置からの、前記コマンドに対する応答時間を計測する計測ステップ
20 と、
前記認証ステップでの認証結果、および前記計測ステップの処理で計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップと
を含むことを特徴とする情報処理方法。
- 25 4. 受信装置との間で共有する共有データに基づいて認証データが生成された後の、応答を要求するコマンドの前記受信装置に対する送信を制御するコマンド送信制御ステップと、

前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づく前記受信装置の認証を制御する認証制御ステップと、
前記受信装置からの、前記コマンドに対する応答時間の計測を制御する計測制御ステップと、

- 5 前記認証制御ステップでの認証結果、および前記計測制御ステップの処理で計測された応答時間に基づく、前記受信装置に対するデータの送信可否の判定を制御する判定制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

- 10 5. 受信装置との間で共有する共有データに基づいて認証データが生成された後の、応答を要求するコマンドの前記受信装置に対する送信を制御するコマンド送信制御ステップと、

前記共有データに基づいて生成された期待値と、前記受信装置において生成された前記認証データに基づく前記受信装置の認証を制御する認証制御ステップと、

- 15 前記受信装置からの、前記コマンドに対する応答時間の計測を制御する計測制御ステップと、

前記認証制御ステップでの認証結果、および前記計測制御ステップの処理で計測された応答時間に基づく、前記受信装置に対するデータの送信可否の判定を制御する判定制御ステップと

- 20 を含む処理をコンピュータに実行させることを特徴とするプログラム。

6. 送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置において、

- 25 前記送信装置から前記コマンドが送信されてくる前に、前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成手段と、

前記送信装置から前記コマンドが送信されてくる前に、前記認証データ生成手段により生成された前記認証データを含む、前記コマンドに対する応答メッセー

ジを生成する応答メッセージ生成手段と、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージを前記送信装置に送信する送信手段と

を備えることを特徴とする情報処理装置。

5 7. 前記共有データは、疑似乱数であり、

前記疑似乱数は、前記コマンドの前に前記送信装置から送信され、

前記認証データ生成手段は、前記疑似乱数に対して鍵付きハッシュ処理を施し、その結果得られたハッシュ値を前記認証データとする

ことを特徴とする請求の範囲第6項に記載の情報処理装置。

10 8. 前記認証データ生成手段は、前記疑似乱数と前記情報処理装置固有の情報に対して、鍵付きハッシュ処理を施し、その結果得られたハッシュ値を前記認証データとする

ことを特徴とする請求の範囲第7項に記載の情報処理装置。

15 9. データの送信可否を判定するのに、前記送信装置から、前記コマンドが最大N回送信されてくる場合において、

前記認証データ生成手段は、前記送信装置から最初の前記コマンドが送信されてくる前に、前記共有データに対して前記処理を施して、送信されてくるN個の前記コマンドのそれぞれに対応するN個の前記認証データを生成し、

20 前記送信手段は、N個の前記認証データが、前記送信装置と予め合意した順番で前記送信装置に提供されるように、前記応答メッセージ生成手段により生成された前記応答メッセージを前記送信装置に送信する

ことを特徴とする請求の範囲第6項に記載の情報処理装置。

25 10. 前記認証データ生成手段は、前記共有データに対して前記処理を施して得られたデータを複数個に分割し、分割されたデータからN個の前記認証データを生成する

ことを特徴とする請求の範囲第9項に記載の情報処理装置。

11. 前記認証データ生成手段は、前記共有データに対して前記処理を繰り返す

施し、その処理毎に得られたデータから、N個の前記認証データを生成することを特徴とする請求の範囲第9項に記載の情報処理装置。

12. 前記送信手段は、前記送信装置からの前記コマンドが受信されたとき、前記認証データと前記コマンドに含まれる情報から生成された新たな認証データを
5 含む応答メッセージを、前記送信装置に送信する

ことを特徴とする請求の範囲第6項に記載の情報処理装置。

13. 送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信可能な情報処理装置の情報処理方法において、
10

前記送信装置から前記コマンドが送信されてくる前に、前記共有データに対して所定の処理を施して、前記認証データを生成する認証データ生成ステップと、

- 前記送信装置から前記コマンドが送信されてくる前に、前記認証データ生成ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージを生成する応答メッセージ生成ステップと、
15

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記応答メッセージを前記送信装置に送信する送信ステップと

を含むことを特徴とする情報処理方法。

14. 送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信するためのプログラムであって、
20

前記送信装置から前記コマンドが送信されてくる前の、前記共有データに対して所定の処理を施しての前記認証データの生成を制御する認証データ生成制御ステップと、

- 前記送信装置から前記コマンドが送信されてくる前の、前記認証データ生成制御ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、
25

前記送信装置から送信されてきた前記コマンドが受信されたときの、前記応答メッセージの前記送信装置に対する送信を制御する送信制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

- 5 15. 送信装置と共有する共有データから生成された認証データに基づく認証結果、および前記送信装置からの所定のコマンドに対する応答時間に基づいてデータの送信可否を判定する前記送信装置と通信するためのプログラムであって、

前記送信装置から前記コマンドが送信されてくる前の、前記共有データに対して所定の処理を施しての前記認証データの生成を制御する認証データ生成制御ステップと、

前記送信装置から前記コマンドが送信されてくる前の、前記認証データ生成制御ステップの処理で生成された前記認証データを含む、前記コマンドに対する応答メッセージの生成を制御する応答メッセージ生成制御ステップと、

- 15 前記送信装置から送信されてきた前記コマンドが受信されたときの、前記応答メッセージの前記送信装置に対する送信を制御する送信制御ステップと
を含む処理をコンピュータに実行させることを特徴とするプログラム。

16. 受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成手段と、

- 20 前記コマンド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信手段と、

前記コマンドに対する受信装置からの応答を受信する応答受信手段と

前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基づいて前記受信装置を認証する認証手段と、

前記受信装置からの、前記コマンドに対する応答時間を計測する計測手段と、

- 25 前記認証手段による認証結果、および前記計測手段により計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定手段と
を備えることを特徴とする情報処理装置。

17. 前記コマンド送信手段は、データの送信可否を判定するのに、前記コマンドを最大 k 回送信し、

前記認証手段は、前記コマンドの送信の順番に応じた前記認証データとその前記期待値とに基づいて、前記受信装置を認証する

5 ことを特徴とする請求の範囲第16項に記載の情報処理装置。

18. 受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、

前記コマンド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信ステップと、

10 前記コマンドに対する受信装置からの応答を受信する応答受信ステップと、

前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基づいて前記受信装置を認証する認証ステップと、

前記受信装置からの、前記コマンドに対する応答時間を計測する計測ステップと、

15 前記認証ステップの処理での認証結果、および前記計測ステップにより計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップと

を含むことを特徴とする情報処理方法。

19. 受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、

20 前記コマンド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信ステップと、

前記コマンドに対する受信装置からの応答を受信する応答受信ステップと、

25 前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基づいて前記受信装置を認証する認証ステップと、

前記受信装置からの、前記コマンドに対する応答時間を計測する計測ステップと、

前記認証ステップの処理での認証結果、および前記計測ステップにより計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップと

- 5 を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

20. 受信装置との間で共有するデータをもとに、コマンド認証データと、応答期待値データを生成する認証データ生成ステップと、

前記コマンド認証データを含み、応答を要求するコマンドを前記受信装置に送信するコマンド送信ステップと、

- 10 前記コマンドに対する受信装置からの応答を受信する応答受信ステップと、

前記応答期待値と、前記受信装置から受信した前記応答に含まれる応答認証データに基づいて前記受信装置を認証する認証ステップと、

前記受信装置からの、前記コマンドに対する応答時間を計測する計測ステップと、

- 15 前記認証ステップの処理での認証結果、および前記計測ステップにより計測された応答時間に基づいて、前記受信装置に対するデータの送信可否を判定する判定ステップと

を含む処理をコンピュータに実行させることを特徴とするプログラム。

- 20 21. 所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置において、

前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成手段と、

- 25 前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成手段により生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証手段と、

前記認証手段による認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信手段と

を備えることを特徴とする情報処理装置。

22. 所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置の情報処理方法において、

前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、

- 10 前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成ステップの処理で生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証ステップと、

前記認証ステップの処理での認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信ステップと

- 15 を備えることを特徴とする情報処理方法。

23. 所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置の情報処理用のプログラムであって、

前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値

- 20 データおよび応答認証データを生成する生成ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成ステップの処理で生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証ステップと、

- 25 前記認証ステップの処理での認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録され

ている記録媒体。

24. 所定のコマンドに対する応答時間に基づいて送信データの送信可否を判定する送信装置と通信可能な情報処理装置の情報処理用のプログラムであって、

5 前記送信装置との間で共有する共有データから、前記送信装置において前記共有データから生成された前記コマンドの認証データに対応するコマンド期待値データおよび応答認証データを生成する生成ステップと、

前記送信装置から送信されてきた前記コマンドが受信されたとき、前記コマンドに含まれる前記コマンドの認証データと、前記生成ステップの処理で生成された前記コマンド期待値データに基づいて前記送信装置を認証する認証ステップ

10 と、

前記認証ステップの処理での認証結果に基づいて、前記応答認証データを含む応答を前記送信装置に送信する送信ステップとを含む処理をコンピュータに実行させることを特徴とするプログラム。

図1

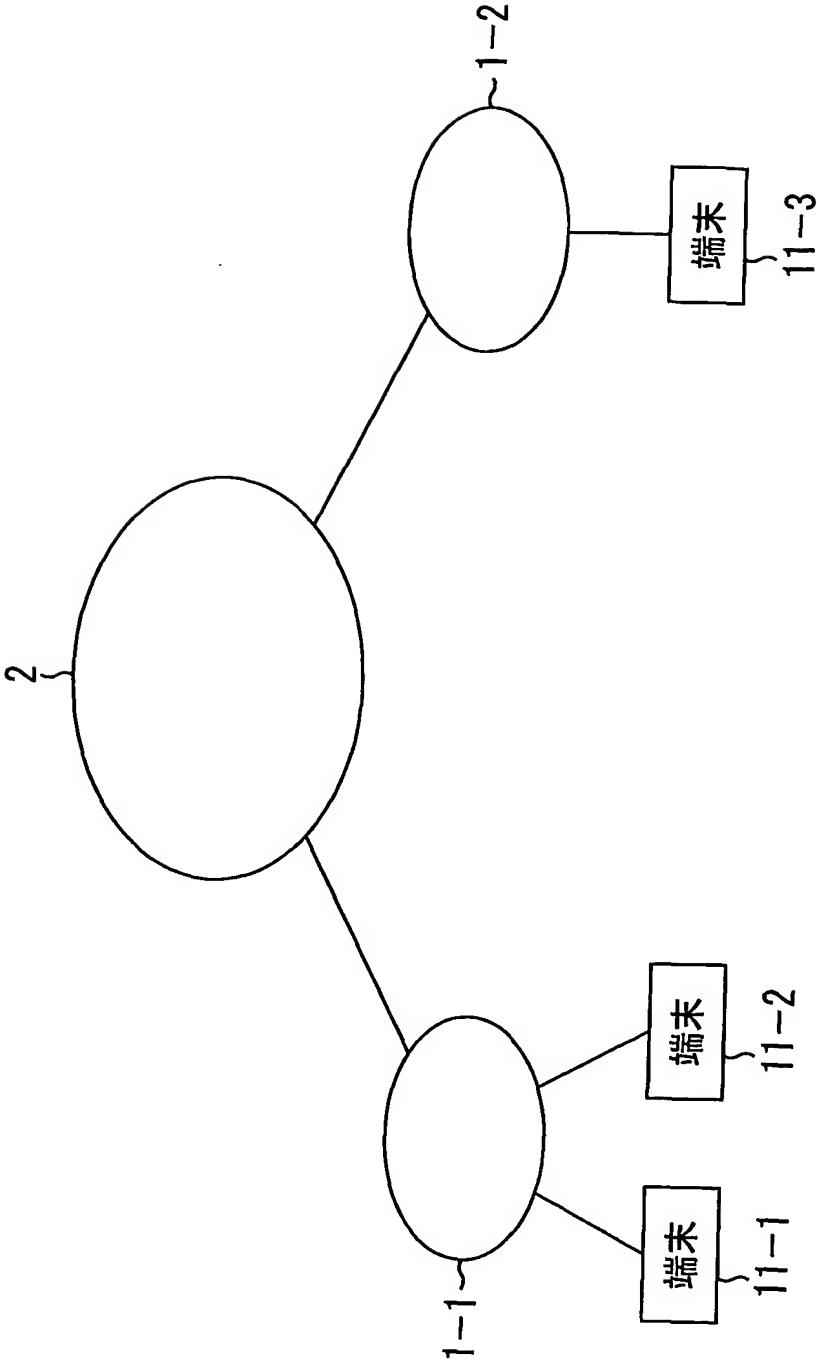


図 2

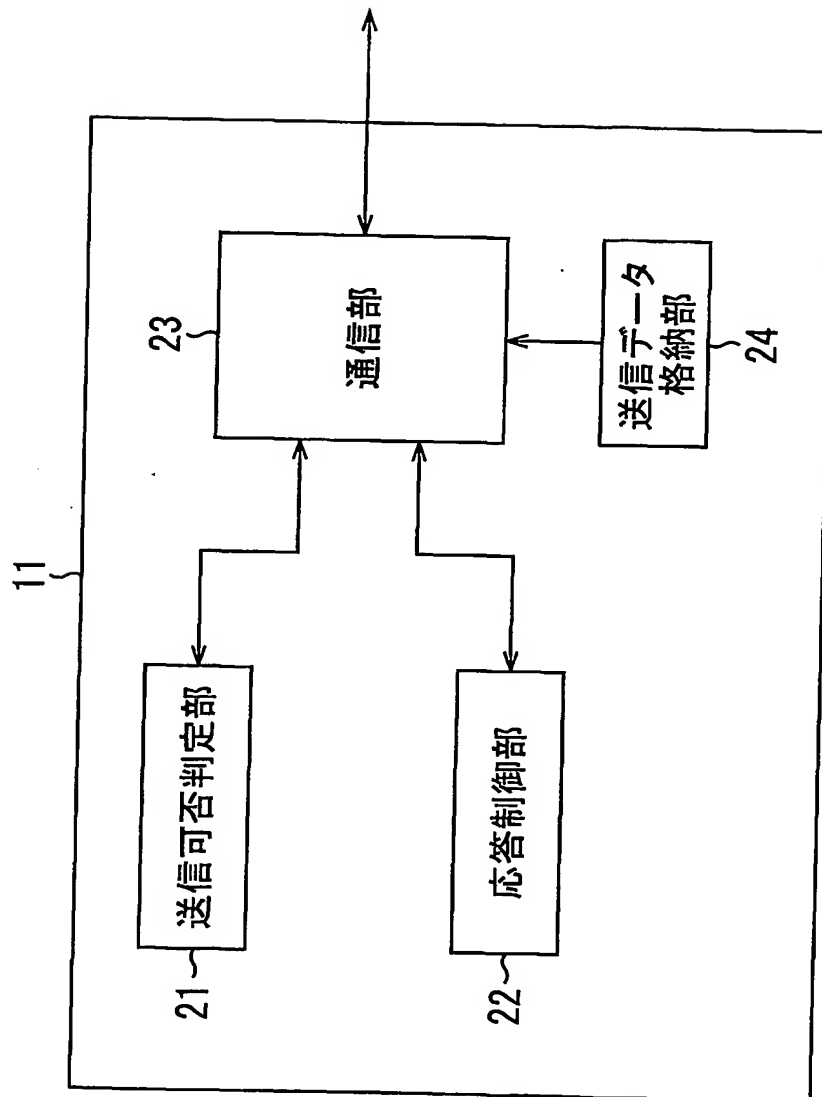


図3

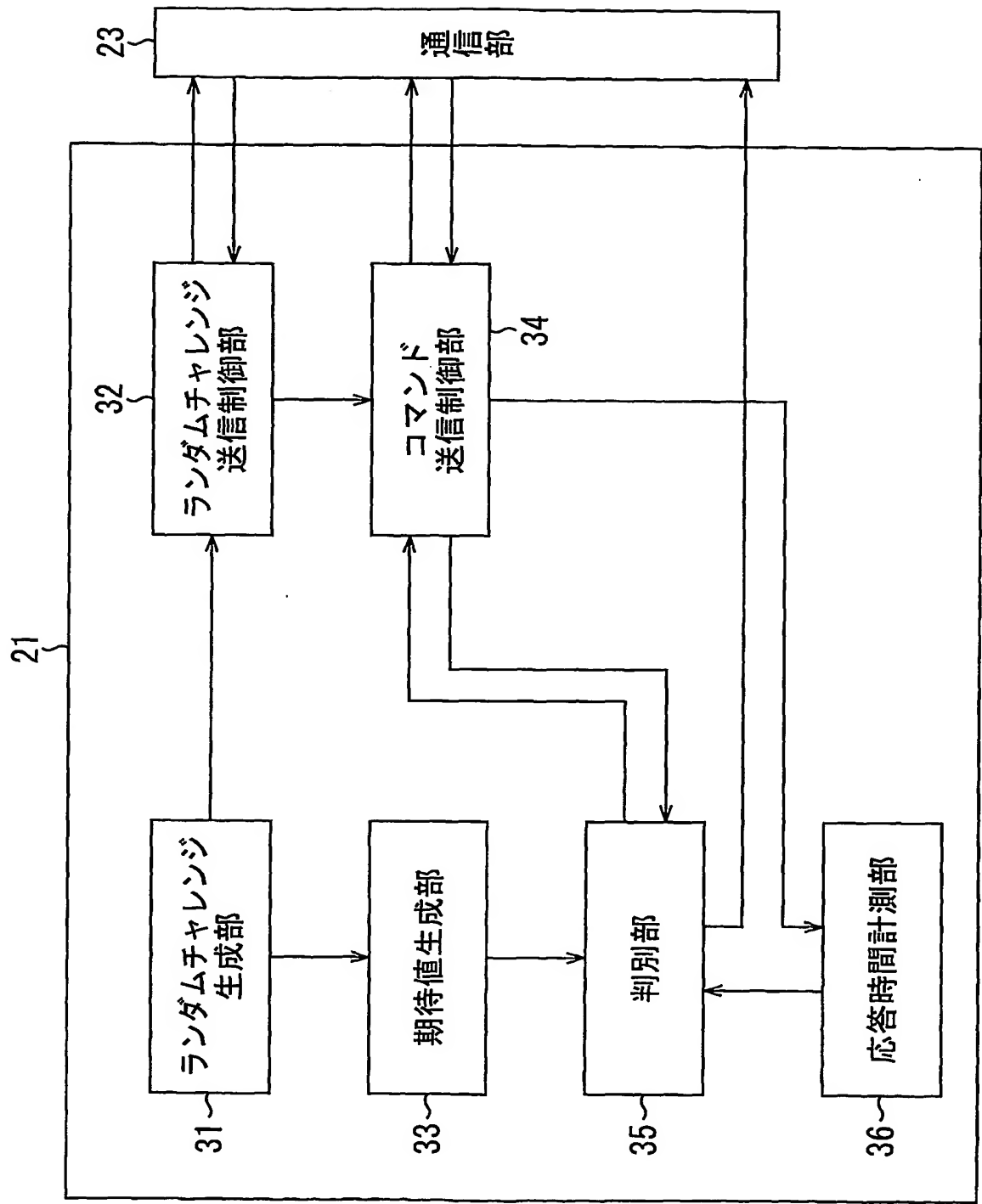
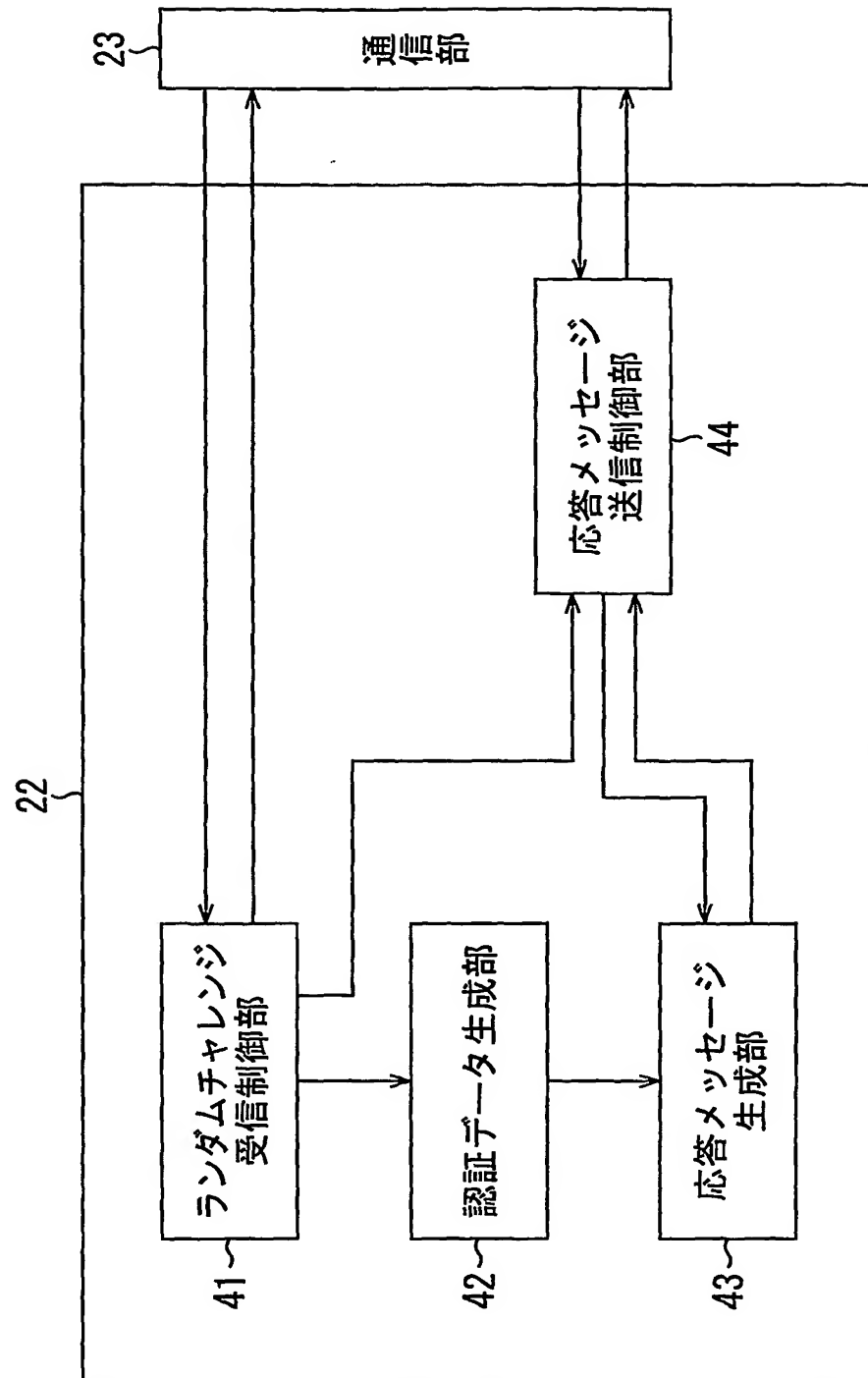


図 4



5/16

図 5

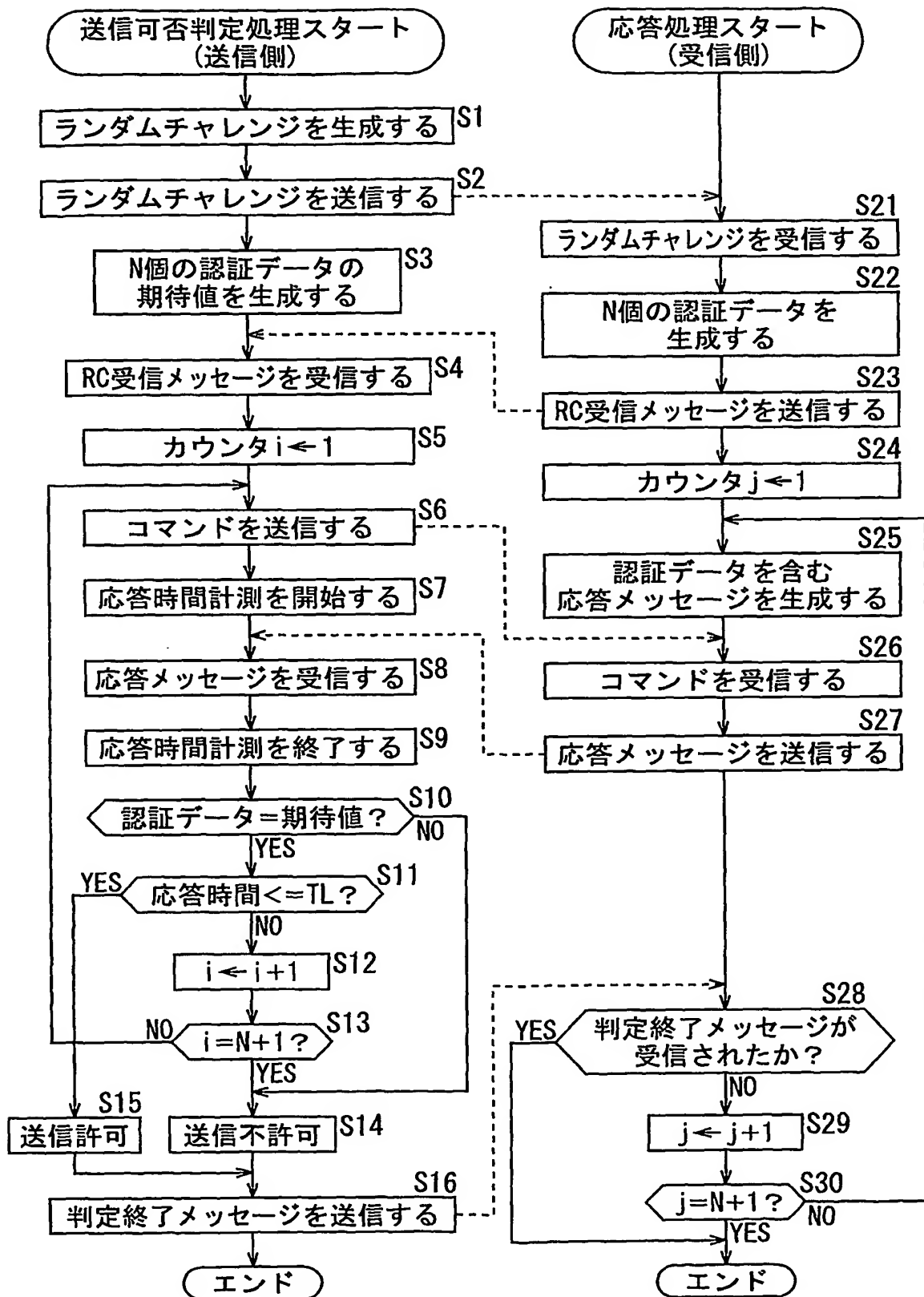


図6

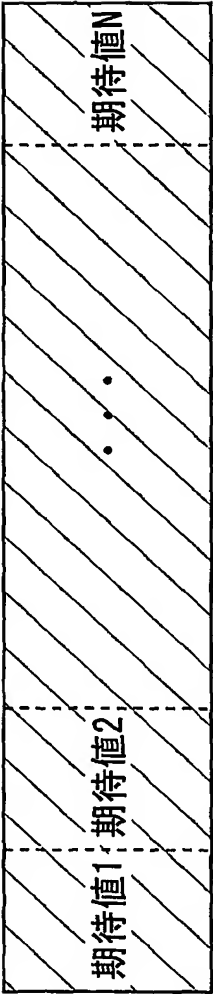
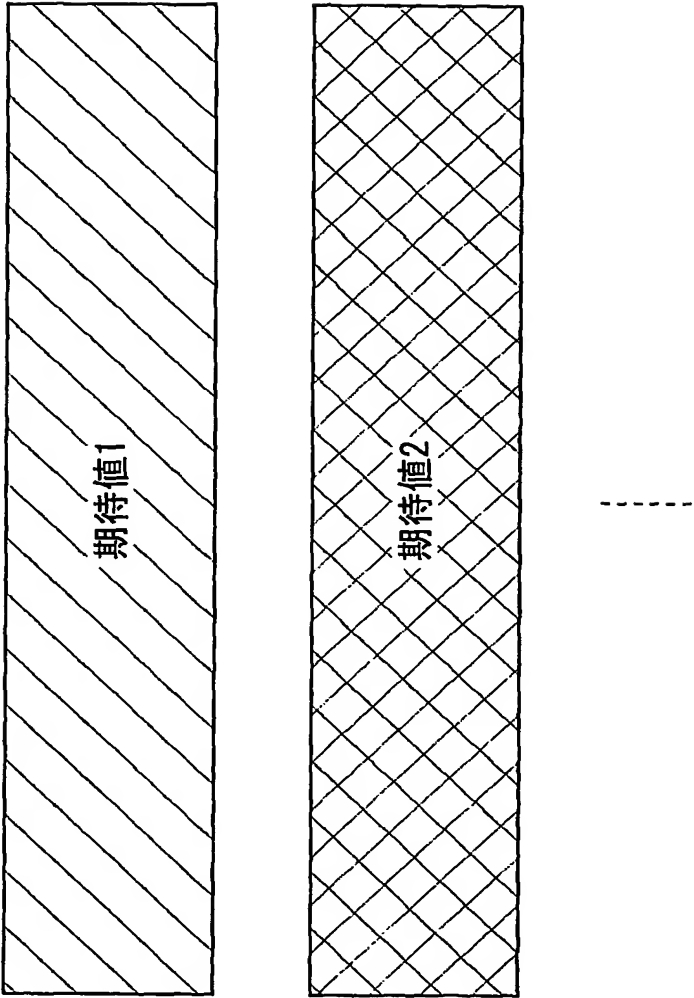


図7



8/16

図 8



図9

21

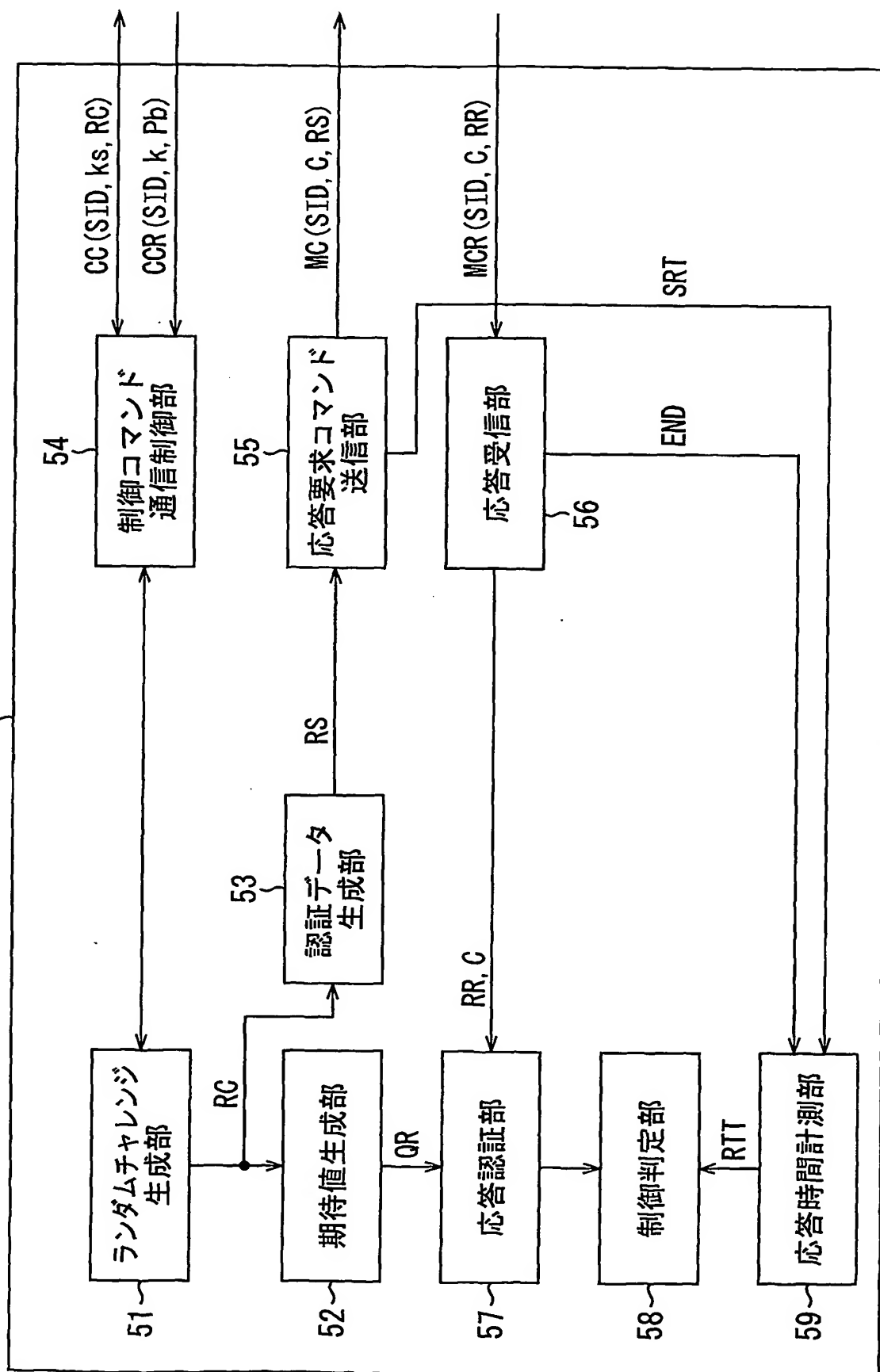
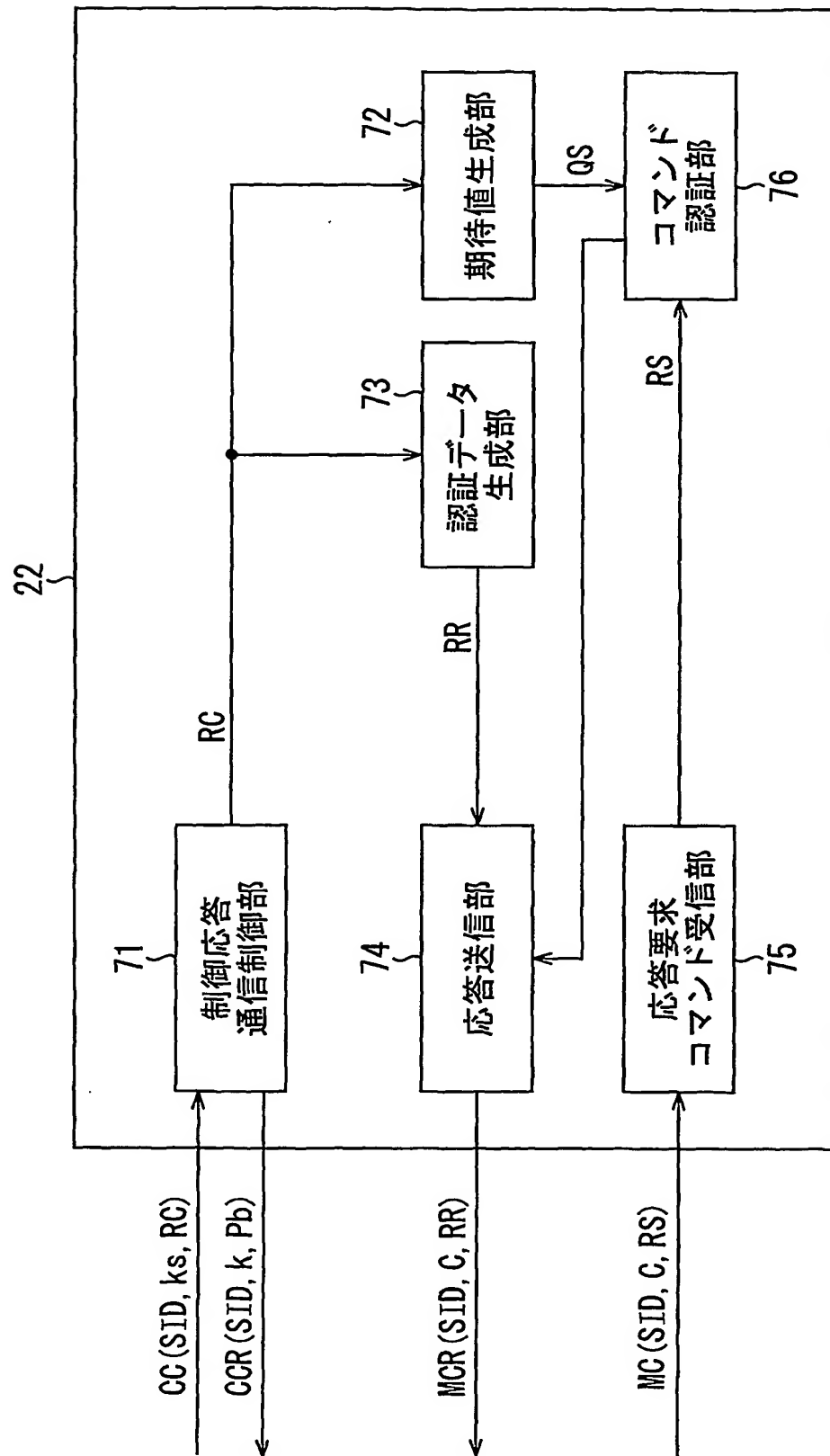
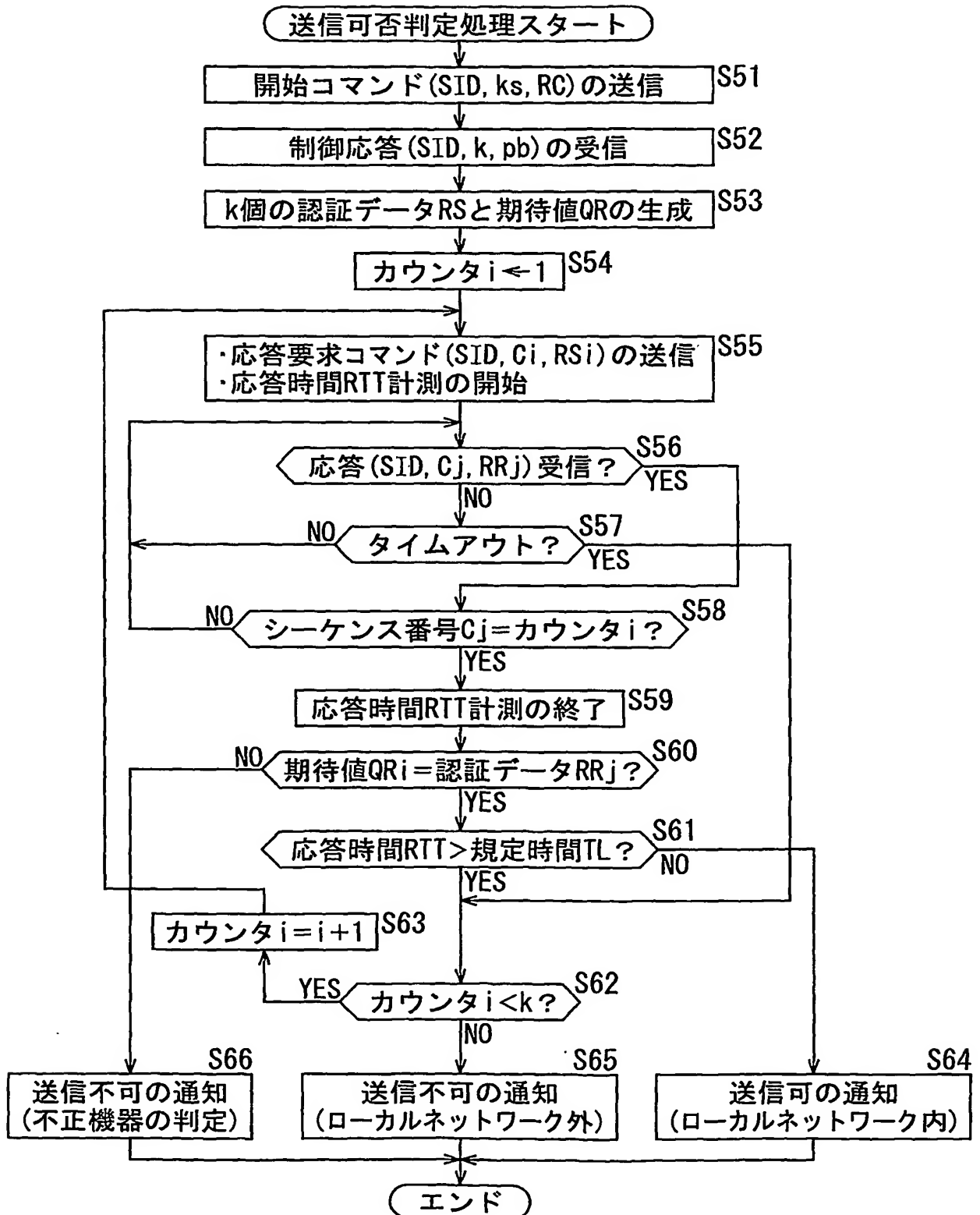


図10



11/16

図11



12/16

図12

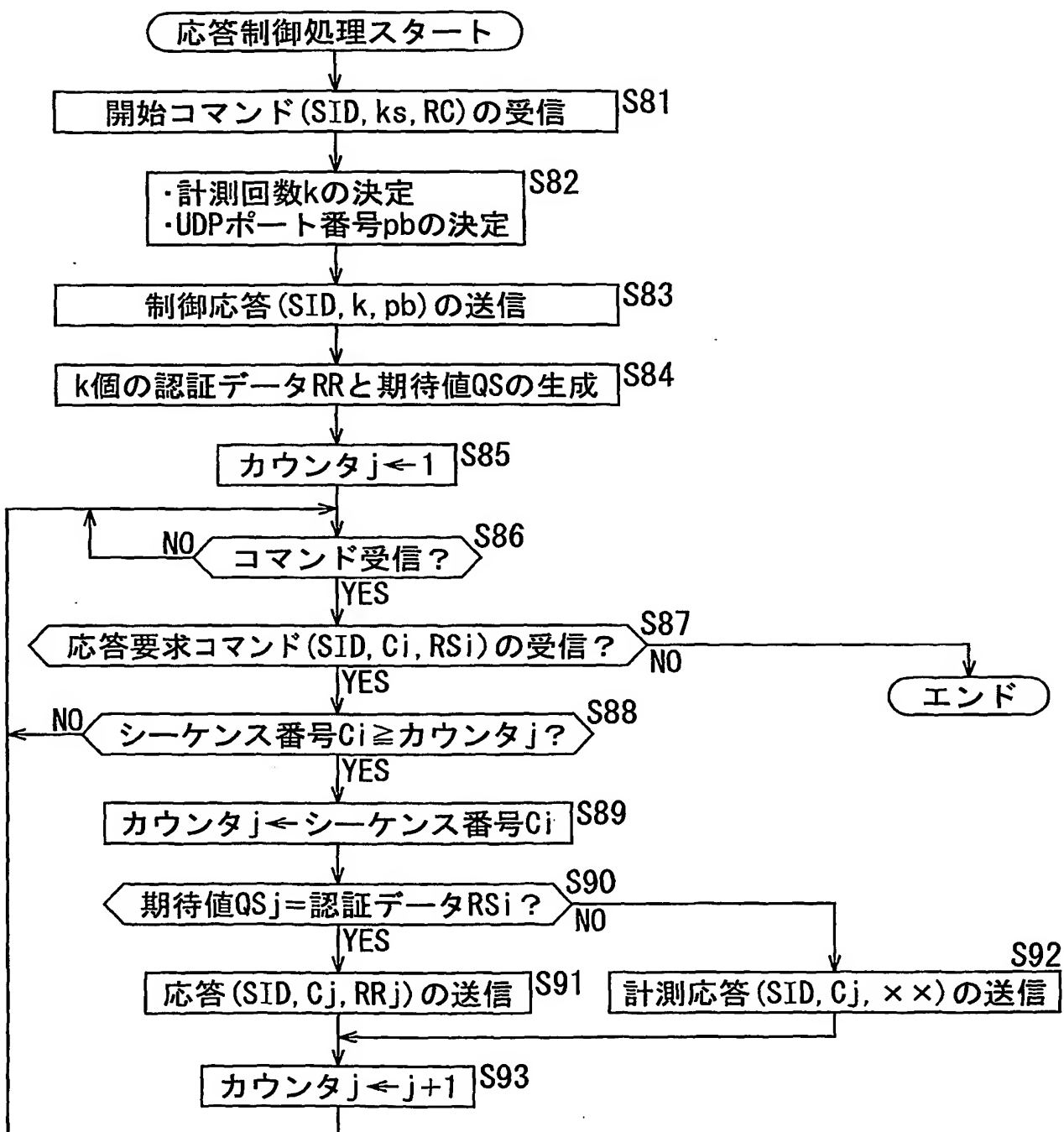


図13

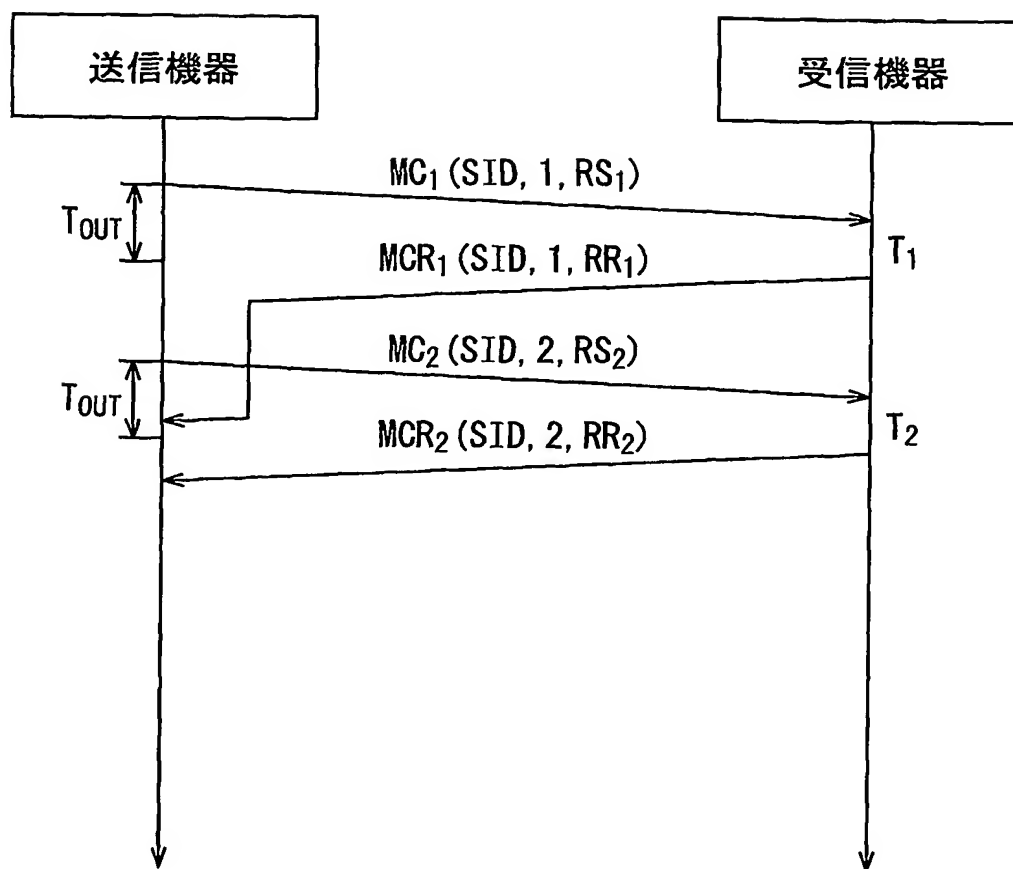


図14

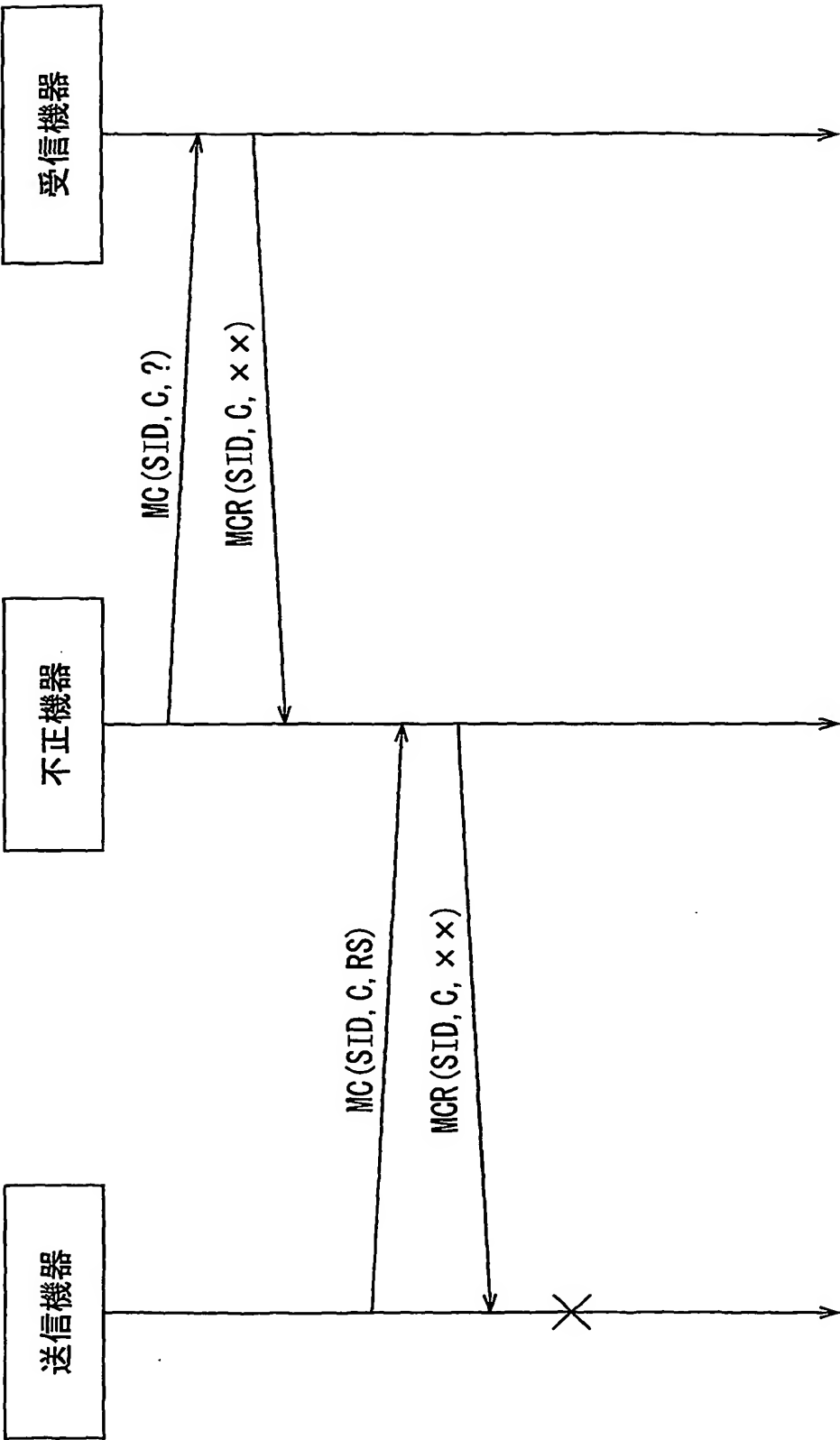


図15

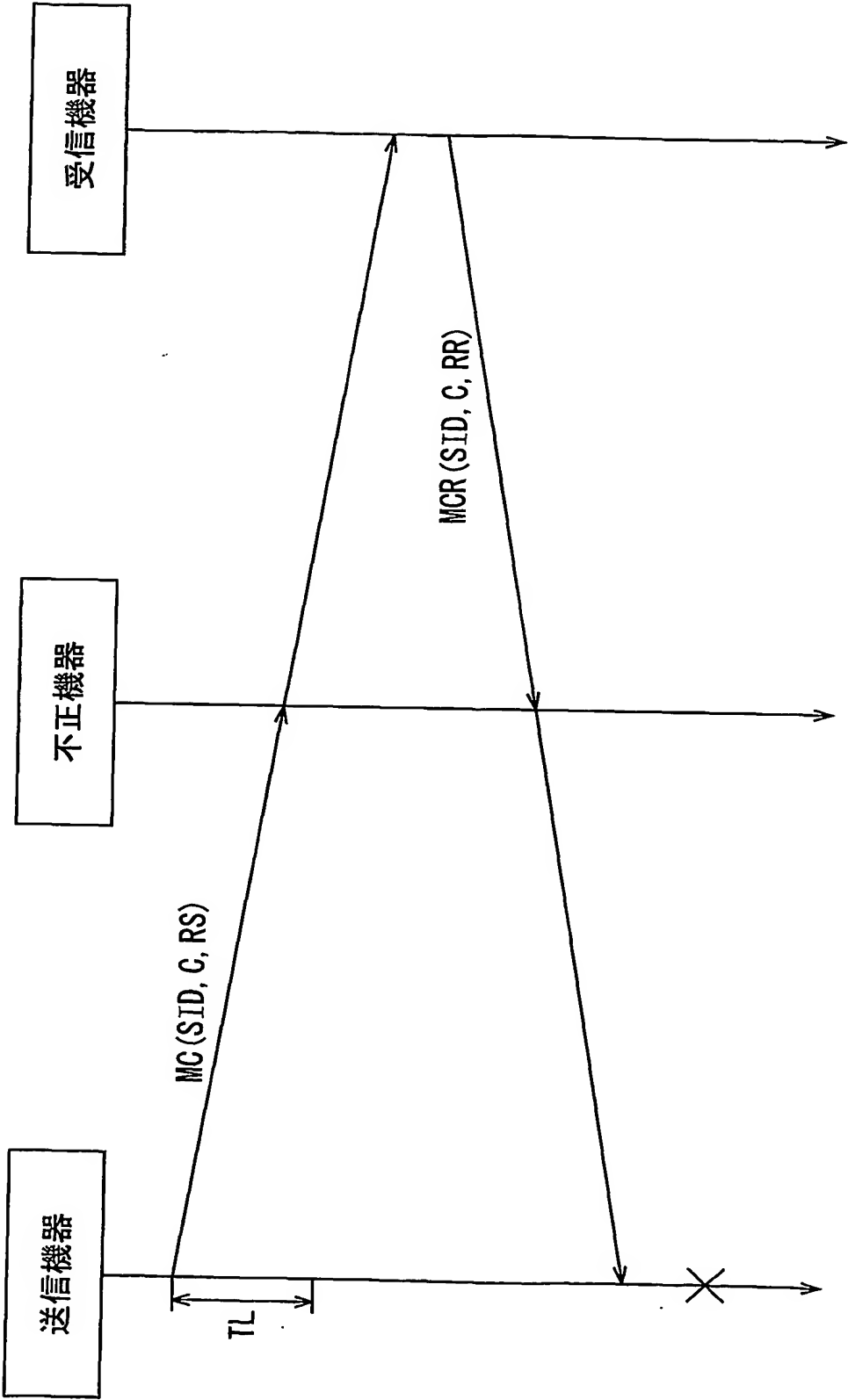
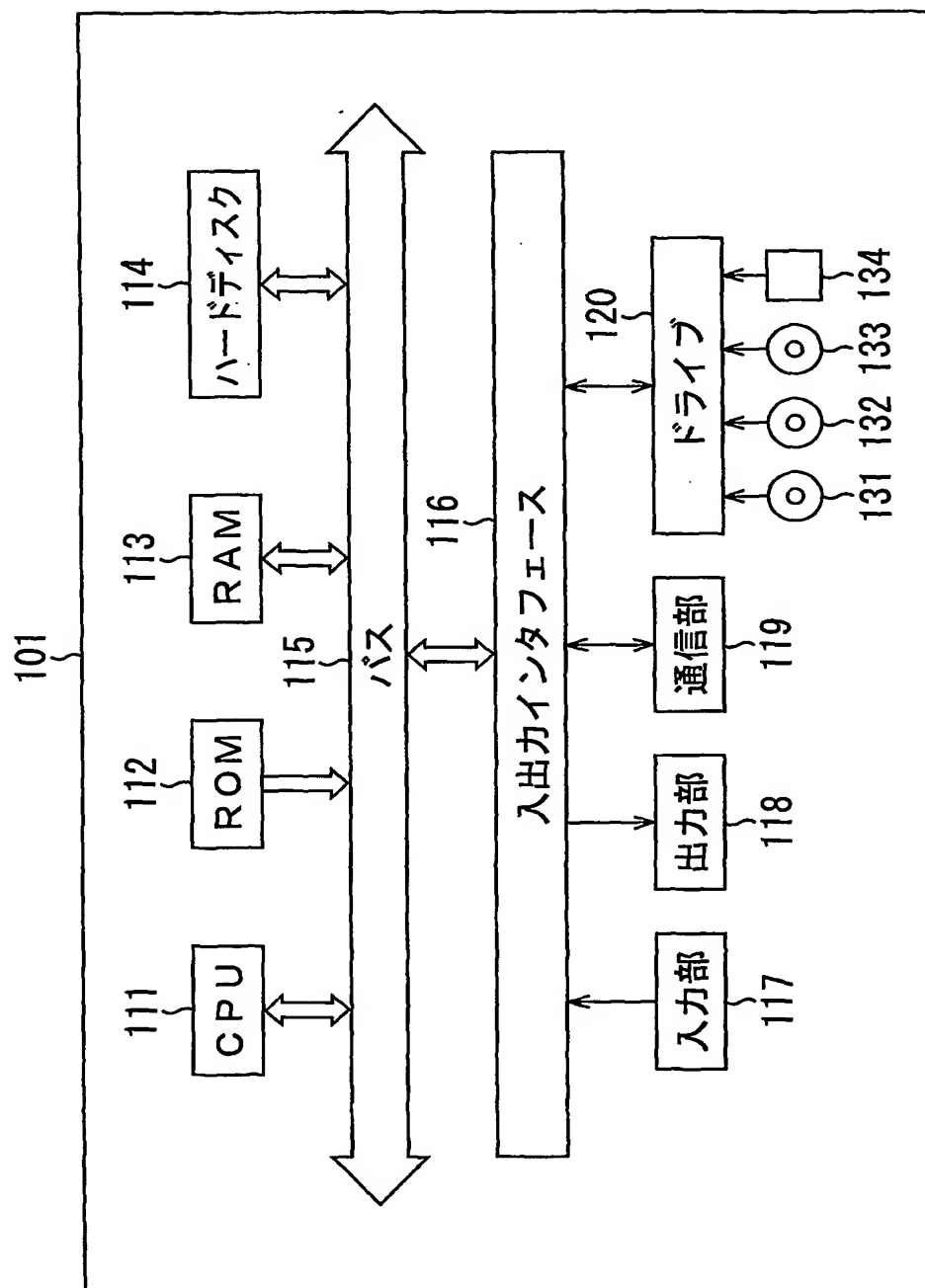


図16



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/009256

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F15/00, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F15/00, H04L9/32, G06F12/14, G06F13/00, H04L12/20

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Toroku Jitsuyo Shinan Koho	1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Ian Fried. 'Apple limits iTunes file sharing'. [online]. CNET News.com.27 May, 2003 (27.05.03), [retrieved on 16 September, 2004 (16.09.04)]. Retrieved from the Internet: <URL: http://news.com.com/2100-1027_3-1010541.html?tag=cd_mh>	1-24
A	Hitachi Ltd. et al. 'Digital Transmission Content Protection Specification Volume 1 Revision 1. 2a (Informational Version)'. [online]. Digital Transmission Licensing Administrator. 25 February, 2002 (25.02.02), [retrieved on 16 September, 2004 (16.09.04)]. Full text, all drawings, Retrieved from the Internet: <URL:http://web.archive.org/web/20030604012332/www.dtcp.com/data/info_dtcp_v1.pdf>	1-24

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
16 September, 2004 (16.09.04)Date of mailing of the international search report
05 October, 2004 (05.10.04)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/009256

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Hachiro ENDO, 'Butsuryu Man no Tameno Pasokon Katsuyo Jissen Koza-96- Network Settei no Kakunin Hoho', MATERIAL FLOW, Kabushiki Kaisha Ryutsu Kenkyusha, 01 June, 2002 (01.06.02), Vol.43, No.5, page 125	1-24
A	JP 11-203249 A (Fuji Xerox Co., Ltd.), 30 July, 1999 (30.07.99), Full text; all drawings (Family: none)	1-24

A. 発明の属する分野の分類 (国際特許分類 (IPC))			
Int. C17 G06F15/00, H04L9/32			
B. 調査を行った分野			
調査を行った最小限資料 (国際特許分類 (IPC))			
Int. C17 G06F15/00, H04L9/32, G06F12/14, G06F13/00 H04L12/20			
最小限資料以外の資料で調査を行った分野に含まれるもの			
日本国実用新案公報 1922-1996年 日本国公開実用新案公報 1971-2004年 日本国実用新案登録公報 1996-2004年 日本国登録実用新案公報 1994-2004年			
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)			
C. 関連すると認められる文献			
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号	
A	Ian Fried.'Apple limits iTunes file sharing'. [online]. CNET News.com. 2003. 05. 27. [retrieved on 2004-09-16]. Retrieved from the Internet: <URL: http://news.com.com/2100-1027_3-1010541.html?tag=cd_mh>	1-24	
A	Hitachi Ltd. 他.'Digital Transmission Content Protection Specification Volume 1 Revision 1.2a (Informational Version)'. [online]. Digital Transmission Licensing Administrator. 2002. 02. 25. [retrieved on 2004-09-16]. 全文, 全図 Retrieved from the Internet:	1-24	
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。			
* 引用文献のカテゴリー		の日の後に公表された文献	
「A」特に関連のある文献ではなく、一般的技術水準を示すもの		「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの	
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの		「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの	
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)		「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの	
「O」口頭による開示、使用、展示等に言及する文献		「&」同一パテントファミリー文献	
「P」国際出願日前で、かつ優先権の主張の基礎となる出願			
国際調査を完了した日 16.09.2004		国際調査報告の発送日 05.10.2004	
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号 100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 宮司 卓佳	5B 9555
		電話番号 03-3581-1101	内線 3545

